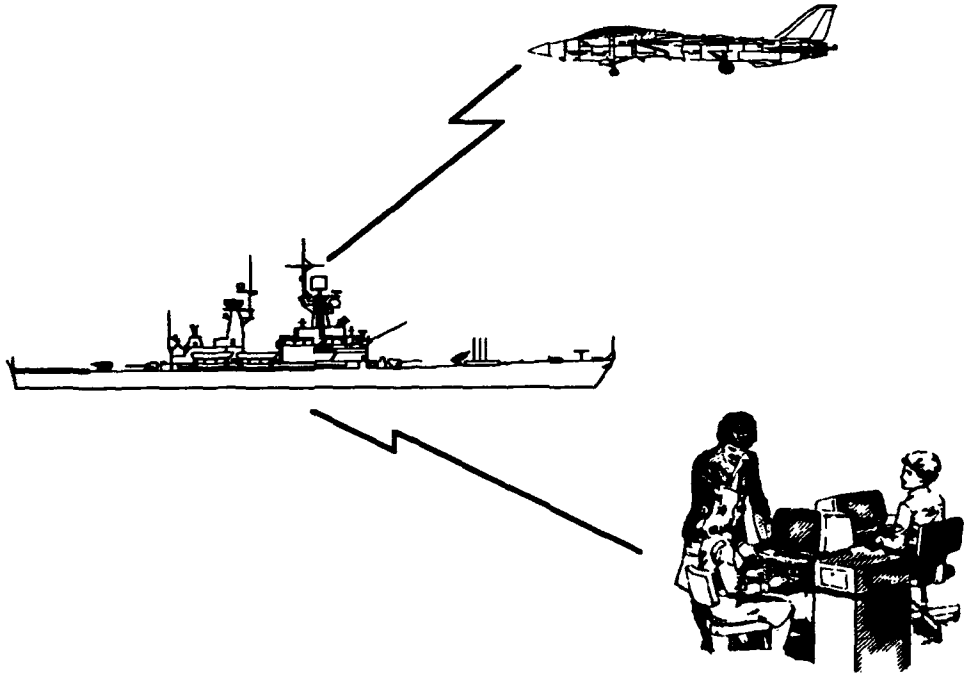
Technical Document 2519
June 1993

Network Security Guideline



NRaD

Technical Document 2519
June 1993

Network Security Guideline

NAVAL COMMAND, CONTROL AND
OCEAN SURVEILLANCE CENTER
RDT&E DIVISION
San Diego, California 92152-5001

K. E. EVANS, CAPT, USN
Commanding Officer

R. T. SHEARER
Executive Director

ADMINISTRATIVE INFORMATION

This document was prepared by the members of the Naval Command, Control and Ocean Surveillance Center (NCCOSC), Research, Development, Test and Evaluation Division (RDT&E DIV) Networking Process Action Team (PAT), at the direction of the Security Quality Management Board. Henceforth NCCOSC RDT&E DIV will be referred to as NRaD.

This document was prepared to assist in understanding how the Center will implement the guidance from numerous security regulations for a network environment, and to establish network security policies and guidelines for NRaD.

This document is made up of four chapters and an appendix. Chapter 1 is an introductory chapter. Chapter 2 describes network concepts and standards to novice network managers, AIS security personnel, and network administrators. Chapter 3 describes NRaD Network Security Policy and Chapter 4 provides NRaD network implementors with quick reference figures (with definitions) for network security policy.

Released by
A. Justice, Chairman
NRaD Networking Process
Action Team

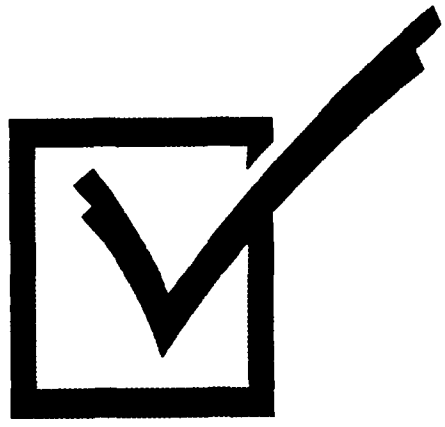
Under authority of
A. E. Walther, CAPT, USN
Executive Officer and Chairman,
Security Quality Management
Board

ACKNOWLEDGMENTS

Appreciation is extended to all of the NRaD Networking PAT personnel who concurrently participated in development of this document from its beginning in March 1991, to end of the assigned task in May 1993. The following Networking PAT members are hereby acknowledged for their tireless efforts in development of this document:

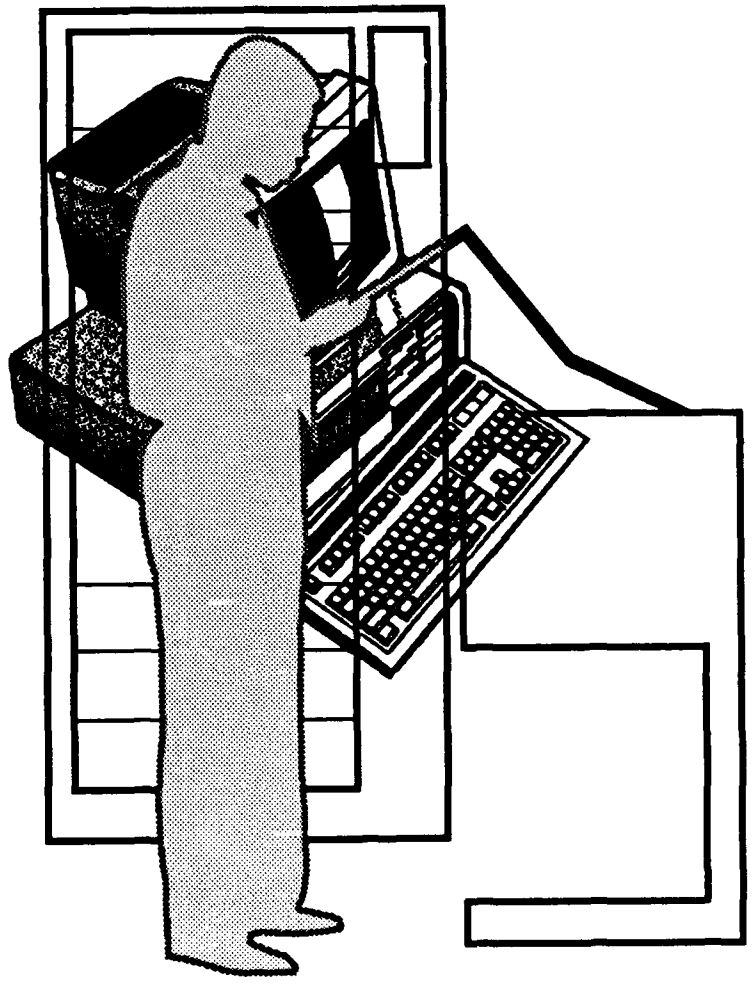
Arthur Justice, Code 41, Chairman
Tom Enderwick, Code 443, Facilitator
Kenneth Boyd, Code 413
Colleen Hiembach, Code 41
Ron Martineau, Code 724
Dave Olsen, Code 465, Editor
Richard A. Fletcher, Head, Code 035
Douglas Kirby, Code 0353
Tom Mattoon, Code 855
Terrence Phillips, Code 913

Table Of Contents



CHAPTER 1

INTRODUCTION



CHAPTER 1

INTRODUCTION

1.1 Purpose

The field of Automated Information Security (AIS) is complex. It involves every security discipline recognized by the Federal Government, Department of Defense (DoD), and U.S. Navy. Numerous directives, instructions, and regulations govern the Center's networking environment. This document was prepared to help you understand how the Center intends to implement the guidance contained in those regulations in a network environment.

It is important for Research and Development (R&D) activities to balance the constraints of existing security policies with the need to explore new technologies and techniques. An R&D environment needs flexibility to experiment with new ideas and approaches that may conflict with existing policies. The purpose of this document is to establish network security policies and guidelines for NRaD. These guidelines provide a standard approach for network security with extensions for operations and yet allow systems to operate outside the constraints of present security policies, where necessary.

This document will also serve as a point of reference when internal and external inspectors review the Center's AIS security program. By publishing these guidelines NRaD can better defend against charges of non-compliance should these circumstances arise.

1.2 Background

In the past, "stovepipe" systems were developed for individual projects. There was little need to share data between systems, and the projects were self-contained. This environment was relatively easy to control since all personnel were cleared to the highest security classification level of the data, and networking was not pervasive. Non-standard technologies further emphasized the segregation between projects. The lack of hardware and software standardization did not support interoperability. Because of the high cost of making changes in proprietary military specified system, changes were slow and methodical. Security policies designed in the mainframe computing world could reasonably be used for assessing the security of a system. These policies were also usually sufficient for avoiding serious problems during inspections or audits from the Inspector General, Navy Audit Service, General Accounting Office, or their representatives.

How the world has changed! No project is an island to itself anymore. All projects are fighting for scarce sponsor funding and all must make maximum use of those resources received by moving to open systems that interoperate with other systems and that offer the warrior a more complete battle picture in a shorter time frame. The Copernicus architecture envisioned by the Navy is fueling this move to a seamless interface among warriors supporting forces and operations. Integrating several networks is easier with more open systems leading to more rapid changes and experimentation.

Modern warfare is often won or lost by the quality and timeliness of the information available to the fighting forces. How to funnel data at multiple security levels and with several different caveats over the same network with acceptable security and performance is a major problem that must be addressed by R&D centers such as NRaD.

The ability to transition to this new open environment is years, if not a decade, ahead of the development of security technologies that can protect these all-encompassing networks. While multilevel security (MLS) networks will someday offer the ability to consolidate data of multiple classifications on the same network and to restrict access according to the individual's security clearance, this technology is not currently an economical solution for most of the Center's needs.

The challenge NRaD faces is to design security policies that provide a reasonable level of assurance against the risks posed to these networks and data given the lack of maturity of the security products. Perfect security is neither affordable nor attainable thus increasing the importance of the risk assessment process.

At best, existing security policies lag behind current technology and industry practice because of the explosive development in networks and the lead time needed to write, approve and distribute new policy. At worst, these outdated policies can slow and sometimes cripple valuable R&D efforts. As the Navy's preeminent Command, Control, Communications and Intelligence center, NRaD is tasked with developing and applying advanced technologies associated with communications networking. While we must be diligent in our protection of classified and sensitive unclassified information carried over our networks, we must not allow outdated security policies to restrict creative and innovative business opportunities, and we must ensure that the service security performs is cost-effective, both in the amount of overhead consumed and in the cost to the user.

1.3 Applicability

These general guidelines are a distillation of a very large and complex set of instructions, directives, and other regulations that bound the AIS security problem. Presented here is what NRaD considers a reasonably balanced subset of those policies, guidelines and instructions.

The manner in which we manage our networks is vitally important to the future of the Center. If classified or sensitive unclassified information is disclosed to unauthorized personnel through unauthorized or unaccredited networks/computer systems, at a minimum the reputation of the Center may be damaged, projects could suffer a loss of sponsor confidence, or national security could possibly be compromised. In the competitive arena that we now find ourselves, such risks must be avoided whenever possible.

For these reasons new networks at NRaD will follow these guidelines unless specific authority to deviate has been granted by the Automated Data Processing Security Officer (ADPSO). Where an intentional violation of these guidelines occurs, administrative or disciplinary action will be taken.

There will always be situations when these guidelines cannot practically be met. Fleet commanders, commanders-in-chief, or sponsors may request unique tests and demonstrations of one-of-a-kind technologies or integration demonstrations of various networks on short notice. The Center may initiate short notice demonstrations when potential business opportunities become apparent. A standard operating procedure for security will seldom be acceptable in these cases. Security must be proactive in helping to seize business opportunities for the Center by finding creative security solutions to complex and challenging situations.

In such circumstances it is expected that close consultation among the network security officer (NSO), the department/division automated data processing system security officer (DADPSSO), network security manager (NSM) and the ADPSO will resolve the issue in a manner that optimizes the balance between controls placed on the network and the total costs of such controls.

DADPSSOs and NSO's should periodically review their systems whenever upgrades are considered to evaluate the ability to meet these guidelines as part of the upgrade. Additionally, each re-accreditation of those networks will include an evaluation of the total cost in time and money tc bring the network into compliance. New technology or a change of guidelines may have made it feasible to meet the standards in effect at that time. Networks accredited before adoption of these guidelines are grandfathered into the

best possible compliance. DADPSSOs and NSO's for these grandfathered networks should perform the same periodic reviews mentioned above to determine those situations where meeting the guidelines is considered cost-effective.

1.4 Administration

NRaD ADP Security Officer (ADPSO) is responsible for administration and maintenance of this document. Contact the ADP Security Officer for further assistance or updates to this document (see Appendix C).

1.5 Existing Security Policies

Figure 1-1

Department of the Navy Security Programs

PROGRAM	APPLICABLE NAVY INSTRUCTIONS
AIS Security	SECNAVINST 5239.2 OPNAVINST 5239.1A TEMPEST - OPNAVINST C5510.93E
Information Security	OPNAVINST 5510.1H
Physical Security	OPNAVINST 5530.14B
Communication Security	OPNAVINST C2200. (SERIES)
TelCom	NAVTELCOMINST C2010. (SERIES)
STU-III	SPAWARINST 2280.2
Industrial Security	OPNAVINST 5540.8 (SERIES)

Figure 1-2

Department of Defense Security Programs

AGENCY	APPLICABLE INSTRUCTIONS
DoD	DoD 5200.28-R DoD 5200.28-M DoD 5200.28-STD
DIS	ISM 5220.22-M
DCA	CSP-1
DIA	DIAM 50-3, 50-4, 50-5
DCID	NO 1/16

DIS - Defense Investigative Service

DCA - Defense Communications Agency

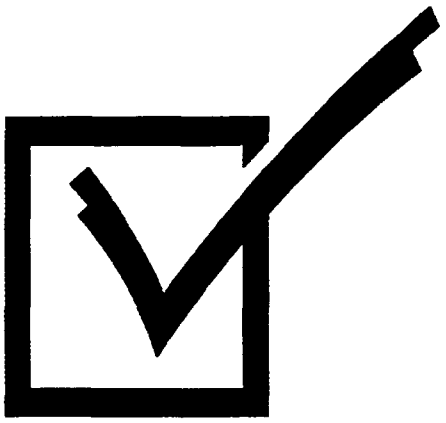
DIA - Defense Intelligence Agency

DCID - Director of Central Intelligence Directive

1.6 Scope

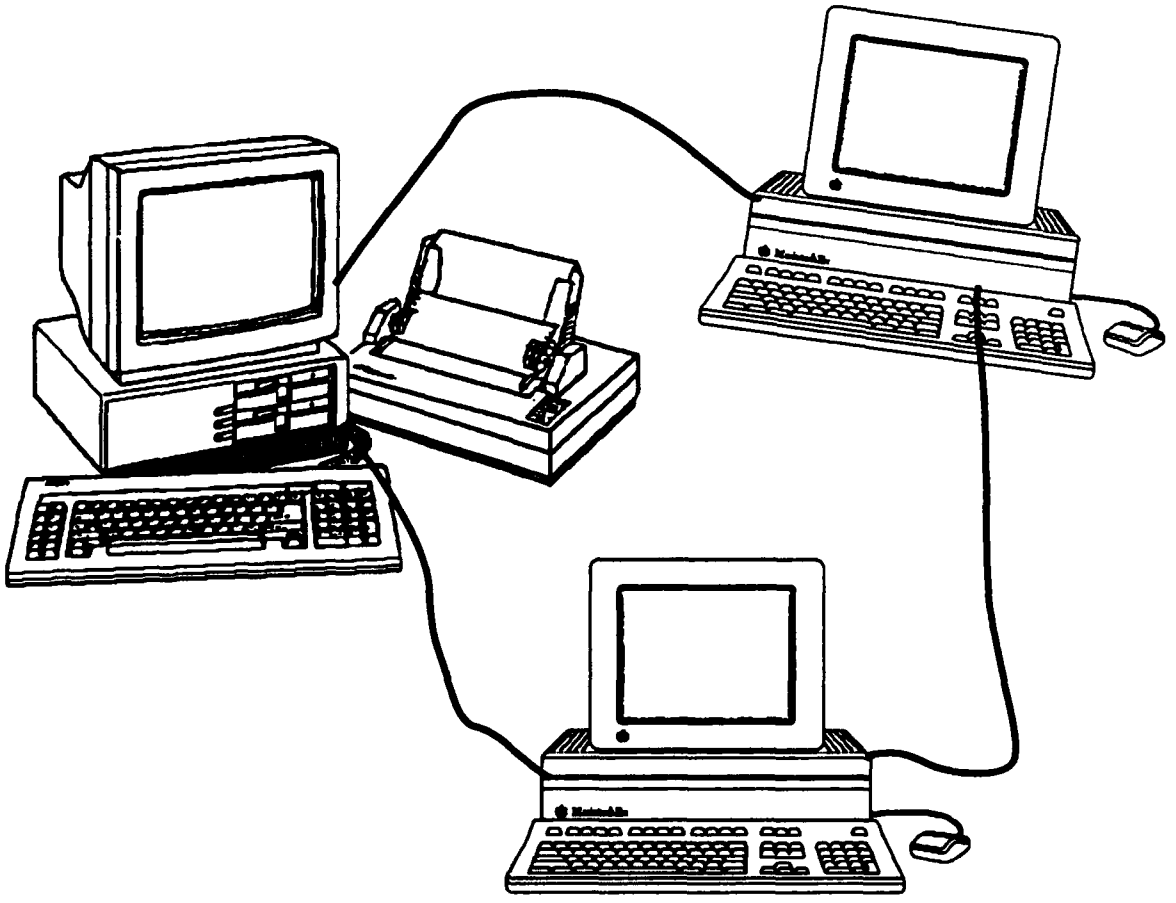
This document discusses and elaborates the general guidelines for the establishment and continuation of networks at NRaD in the following areas:

- Security
  - ◊ Information Security
  - ◊ Computer Security
  - ◊ Communications Security
  - ◊ TEMPEST
  - ◊ Personnel Security
  - ◊ Physical Security
  - ◊ Signal Security
  - ◊ Operations Security
- Installation and Configuration
- Performance
- Management/Administration
- Accounting
- Maintenance



CHAPTER 2

NETWORK ARCHITECTURES AND DEFINITIONS



CHAPTER 2

Basic Network Tutorial

2.0 Purpose

This section is intended to be a basic tutorial on networking and communications as well as a discussion of network security. However, because of space and time limitations, we will not be able to address all of the issues you will need to know when planning your computer communications network. We will try to present a quick overview of some important terms and topics on communicating and protecting information.

For more information about computer networks contact your Department/Division ADPSSO (DADPSSO). Your DADPSSO along with the NRaD Electronic Systems Security Group and the station's Network Security Manager (NSO) will help with compliance with computer security regulations.

2.1 Network Security Discussion

What is network security? Paraphrasing from the Internet Engineering Task Force (IETF)[1], network security is understood to include protection against:

- The loss of privacy of information,
- unauthorized modification,
- denial of service, and
- unauthorized access.

If we were to describe what we would want in a "ideal" secure network, we might ask for a network that would[2]:

- Deliver data only to the destinations specified.
- Ensure that the data will not be modified in transit.
- Protect the data from being disclosed to unauthorized or unintended parties.
- Keep observers from gathering information about data exchange participants or events through traffic analysis.
- Prevent unauthorized parties from masquerading as valid participants.

---

[1] Network Working Group Request For Comments (RFC) 1281 (Guidelines for the Secure Operation of the Internet).

[2] This list was abstracted from "Communications Support System Security Interfaces", NOSC Code 855, Tom Mattoon, dated: 13 Nov. 1991.

- Guarantee that the data has reached its destination.
- Be available when needed.
- Perform within specification for speed and capacity.
- Allow for breaches of security rules to be traceable back to the offending person or process.

We also want the system to be affordable (actually, we want it for free, but we know that the world doesn't work that way). So, we try our best to build security into our network by addressing the requirements for the security level of the data we are trying to protect. Often, we end up with a balancing act of trying to adhere to security regulations[3], meet our requirements to do the job, and still stay within a budget. In other words, if we can't afford it, and if our security risk assessment allows it, we start chopping requirements off of our "ideal" secure network list.

For instance, since NRaD is an RDT&E facility, a particular group might not have an operational requirement to protect their communications from traffic analysis. Since this is an expensive security feature to implement[4], the groups may decide that they can live without it.

In fact, until recently, only a few of the security capabilities on our list were obtainable on a network. The remaining capabilities were functions of a computer operating system, available only for point-to-point links, or not available at all.

As an example, let's look at our first "ideal" secure network feature: "deliver data only to the destination we have specified". Once you put a data packet[5] onto an ethernet LAN segment, everyone on this segment has the potential to see the packet. Fortunately, most of us have computer network devices that adhere to predefined protocol conventions. If everyone is a "good citizen" and follows these conventions, the network works. One agreement that is made between ethernet interface hardware is: "even though I can see every packet on my segment, and will read every address header, I will not read the information in the packet unless it is addressed to me or my group".

Unfortunately, not all vendor's hardware will play by the rules, and there are people (who are not good citizens) who will modify their hardware drivers just to take a peak at things. So, to protect your data from possibly being seen by another machine, you may have to isolate your network segment and have only people on it that you trust to use it.

---

[3] Department of Defense, Department of the Navy, Naval Space and Warfare Systems Command (SPAWAR), and NRaD

[4] Packet encryption is expensive in terms of hardware and software, traffic padding is expensive in terms of wasted capacity and processing time

[5] A data packet is one transmission onto a network, consisting of header information (source and destination addresses), protocol information and typically some sort of data.

Another method you can use is to encrypt your data so that if it is seen, it cannot be understood. Until recently, "network encryption"[6] devices were not available, and the units that are available today are expensive and will exact a performance penalty.

Networks enable computer users to share information and resources. While many security safeguards have been built into computer operating systems, networks are often wide open conduits for passing information.

One reason for this has to do with the relative youth of network technology. While the mainframe computer has been around for over forty years, the concept that a network is more than just a way to access a mainframe with a remote terminal or to transfer data from one mainframe to another is less than fifteen years old (with most of the real work being done in the last seven). With the data explosion caused by the personal computer, large investments have been made in developing the technology to share data through networks. Unfortunately, the technology necessary to protect this information flow has lagged far behind the technology to distribute it.

Mainframes concentrate large amounts of valuable corporate data at centralized locations. Great lengths were taken to protect this information by physically and logically restricting access to the computer and the stored data. Locked doors protected the computer, disk drives and tapes. Username and password schemes were implemented to control access to these computers and their applications to prevent access to data records, fields, or elements. To get permission to access this data, one would have to go to a Management Information Systems (MIS) group (usually the database manager, the computer system manager or one of their agents) to obtain access permission.

Because of the security that was typically in place at the centralized computer center, the need to protect access to the network was not given much thought, except for some industries like banking and defense. With the advent of the personnel computer, however, the need for network security has changed. The "PC" (MAC's are included too) has fostered a new user philosophy that data should be immediately accessible and not locked up behind a glass wall. The idea that the computer and data belong to the user and should no longer be controlled by the Management Information System group (a.k.a. MIS - computer priests and monks in white lab coats who like cold, air-conditioned, glass-enclosed computer rooms) is now the prevailing rule.

A new decentralized view is leading to more and more data being generated and used away from the protected confines of the computer room. Hence, we have the

---

[6] Most "KG" encryption devices work on a point-to-point circuit. These new network capable encryption units (such as the Motorola NES, Xerox XEU or WANG TIU) will allow a node to connect directly to a network or will encrypt a network onto a WAN link or backbone.

greatest driver behind the network revolution - once information has been generated and it is being used by individuals, they find they have a need to share this data with others. Within the Navy and DoD, the same view is being adopted. If information is generated or stored in one location, it must be sharable with those that have a need to use it at another location.

Remember, the network technology that has developed over the years is weak in regards to security. Securing a network was, and still is, expensive. The effort, or the money, was not spent because operational procedures[7] took care of many of our security requirements. Not any more. As an example, how many people do not have usernames and passwords on their PC's or MAC's? Yet, these devices are put on the same networks that others are using to transfer sensitive, or "for government use only", information. It's clear that new thinking about computer/network security is in order.

2.2 Network Design

To understand that we have to think about network security right from the very beginning as part of a design effort, let's look at network architecture in general and what security issues have to be kept in mind when designing or installing a network for a building or workgroup.

Until recently, networks were thought of in terms of Local Area Networks (LAN), Wide Area Networks (WAN). Now, Campus and Metropolitan Area Networks (CAN and MAN) are sneaking into the vocabulary[8]. What is important to realize, is that the boundary distinctions of a LAN, WAN, CAN or MAN are being expanded beyond traditional local or geographic limits to potentially boundless, global networks that can take our communications requirements anywhere. This is great, as long as we can control where our data goes and protect it from getting into the hands of people who do not have a legitimate need to access it.

When designing a network you have to be concerned with:

- bandwidth requirements
- protocols
- security and a host of other details
- physical layout
- applications

[7] Operational procedures such as, batch processing, mailed printouts or magnetic tapes, applications programming under MIS control, data request forms, locked doors, terminal rooms, ...

[8] How about VAN - value added networks, GAN - global area networks, the list goes on.

In this section we will touch on topologies, such as what types of network devices and components are available, what types of cable plants can be run, and what protocols need to be supported.

However, if there are two points that we can get across to you, the network requester, they are that if you want to network you need to: 1) design in security from the very beginning, and 2) lay your foundation on top of recognized standards!

For instance, use ethernet, token ring or FDDI for your LAN connections; IPX/SPX, TCP/IP and ISO/OSI as your protocols; and a POSIX compliant operating system or Novell Netware on your server.

Do not let a vendor push proprietary or even "de facto standard" equipment or protocols on you. Only use proprietary or de facto standards if the capability you need is not covered by an accepted standard body. The extra little bit of money you might save by buying a proprietary solution will, more times than not, cost you far more in a loss of compatibility and future expansion capability.

Novell, MS-DOS, MS Windows and Apple Macintosh are examples of de facto standards that we have to live with. As companies, Novell, Microsoft and Apple are so big that applications developers will either exclusively produce, or will release products for their platforms first. However, as consumers, we should demand that all products adhere to standard network protocols and standard data transfer capabilities.

This chapter will cover some network standards as well as some common "proprietary standards" that are in use at NRaD.

2.2.1 Network Topologies.

When discussing topologies you'll often hear of the terms logical topologies and physical topologies. The difference being that a logical configuration pertains to how one node relates to another in terms of the protocol technology, while a physical topology describes how the cable (or other media) is laid out. Hence, it is possible to have a logical network of one type laid out as a physical configuration of another type. Ah!, clear as mud. Let's try and explain.

2.2.1.1 Logical Topologies

There are five major logical topology types for networking: bus, daisy chain, ring, star and tree.

A **bus** topology is best visualized as a straight data path or "wire" with "nodes" hanging off of it (fig. 2-1a). So, to get from node "A" to node "C" you have to get onto the bus, past the node "B" connection, and then finally off the bus to node "C". This scheme is repeated along its entire length.

A **daisy chain** network is where each node is connected from node-to-node-to-node, and so on (fig. 2-1b). Imagine trying to get from nodes "A" to "C" again. However, this time only two devices are connected to each segment wire and you have a node connecting two segments. With this topology data has to travel to, and be passed on by, node "B".

With a **ring** topology the entire segment length is enclosed to form a circle (fig. 2-1c) so that there are no terminating ends. Ring's typically do not have a master device arbitrating access to the network so they work very much like a logical daisy chain network. Let's go back to our example of getting from node "A" to "C". Most rings will have data traveling from "A" to "B" to "C" and so on back to "A". If "C" needs to respond back to a request from "A", the reply will continue along the same direction as the first message and pass through "D" and "E"; therefore, communications is unidirectional along a segment.

The **logical star** topology has connections that radiate out from a central hub (fig. 2-1d). As an example, nodes "A", "B", and "C" are all connected to a central node, or hub, "X". For a message to get from ether "A", "B", or "C" to one of the others it must always pass through "X".

A **logical tree** topology is often described as a hierarchical network where you have stars (hubs) connected to other stars (hubs) (fig. 2-1e). "A" talks to "C" by first passing its message to hub "Y", then to hub "X", which now communicates (somehow) to hub "Z", which finally passes its message to "C".

The final logical topology we are going to cover is the **switch** (fig. 2-1f). There are two types of switches used in networking. One type keeps the circuit path connected throughout the duration of the call, such as a telephone PBX. The other type is when the connection is in existence only for the time needed for that data packet to pass through, as an ETHERNET switch or cell-relay switch. The logical operation of a switch can be compared to a star hub ("A" gets to "B" by passing through "S"), but where a logical

star will often repeat the signal to every connection, a switch will only send data down the wire segment to the target device.

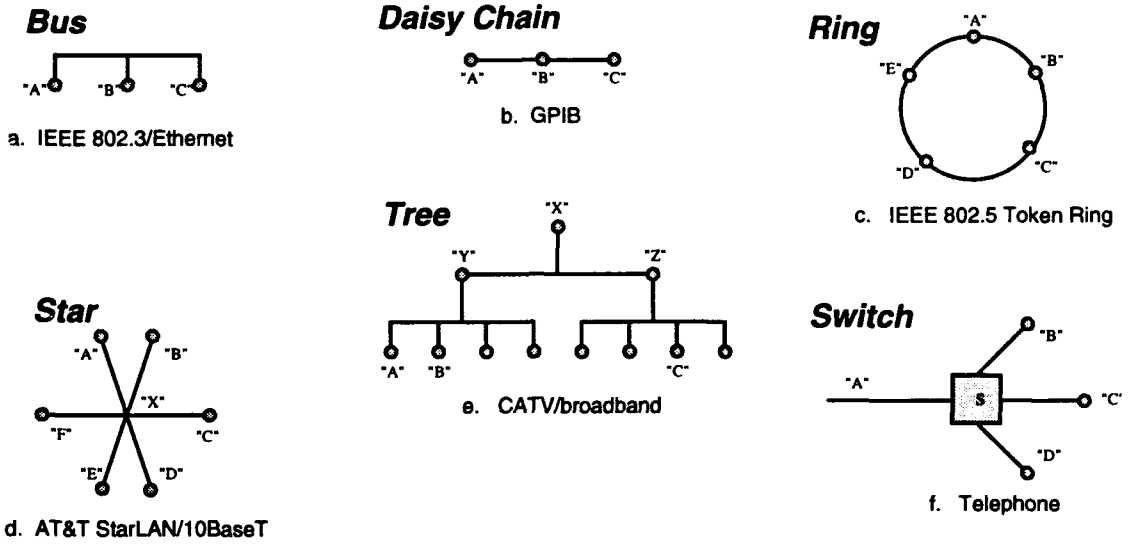


Figure 2-1
Network Topologies

2.2.1.2 Physical Topologies

Physical topologies have many of the same descriptive names as the logical topologies (bus, ring, star, tree, etc.). Except that the emphasis is now with the physical appearance, or configuration of the network, not the "logical" protocol interconnection scheme.

Think of a **physical bus** topology as a long cable strand (doesn't have to be straight) where one connection is placed after another. So, when wiring up an office or lab with this topology, the network cable has to travel close to each node and have a tap line connecting to it. An example of this is thickwire ethernet with a transceiver cable connecting to the main segment). Another method used is for the wires to make their way directly to a node, and away to the next node. An example of this is thinwire ethernet, where the cable daisy chains from "t" connector to "t" connector.

For the **physical ring**, the layout of the media forms a ring, running from one device, to another, and so on, until the first device is connected again. As far as the wiring in the office goes, the link is usually a daisy chain where the upstream wire has to be run to the node being connected, and then another wire is run to the downstream device.

With a **physical star** topology, the media will be run from a central location (though it doesn't need to be connected to a central node). The advantage of star configurations is that the length of individual runs are less than a bus or ring physical segment. This helps with timing and signal levels and with troubleshooting a run since the cable is typically run directly from the hub to the device. The disadvantage of this method is that the total length of cable used is greater (one cable length per device). There is also a large concentration of wires being run to the hub.[9]

Trees are normally multipoint segments connected to other multipoint segments in a tree pattern, or in other words, hubs connected to hubs, switches connected to switches, or any configuration where wiring from a concentration point branches to other concentration points or network nodes.

For an example of a logical topology that is laid out in a different physical configuration, look at a logical ring that is hubbed as a star to a central wiring location. An example of this is an FDDI ring connecting to station nodes via a concentrator. Fiber cables are "home run" from the devices being connected to the concentrator, but information travels from device to device as though the hub doesn't exist, and all of the attachments where made directly to the ring.

2.2.2 Network Media

The next step in designing a network is to decide what type of physical media is going to be used.[10] The current major technologies in network media are:

Fiber Optics	Coaxial Cable
Twisted Pair	Wireless

Each has advantages and disadvantages. For instance, fiber optic cable is perhaps the most secure and has the greatest bandwidth potential. It is also the most expensive to use for a LAN. Twisted pair is becoming the cheapest and it is easiest to work with during installation, but has bandwidth problems and a particularly nasty tendency of picking up noise and radiating signals at higher frequencies.

Selection of media type usually comes down to looking at the media requirements for the network technology to be selected (e.g. ETHERNET, FDDI, Phonetalk, etc.); cost of the media, network devices, host connections and installation; and sometimes security considerations.

---

[9] Typically hubs are hidden out of sight because of the huge, ugly bundles of cable running to them.

[10] Actually, the process of selecting the topology, media type, network devices, and network technology is usually made at the same time due to performance requirements and cost considerations.

Fiber Optics

Fiber-optic cable has several security advantages over most alternatives. Fiber-optic cable is immune to Electromagnetic Interference (EMI) so transmissions cannot be "jammed" or corrupted by high power emitters such as radio transmitters. Fiber optics do not emit Electromagnetic Radiation (EMR) and thus avoids being snooped with an antenna. Splicing into a fiber-optic cable for the purpose of eavesdropping is difficult and can be easily detected at the receiving station as an decrease in signal strength. Attempts, to tap fiber is easier to detect with visual inspection of the cable due to the multiple layers of cable jacket and strength materials that have to be removed before bare glass is reached.

Fiber-optic cable is also safer to use than copper. Since no electronic current can pass through the cable, no ground potential differences can be created from one end to the other.

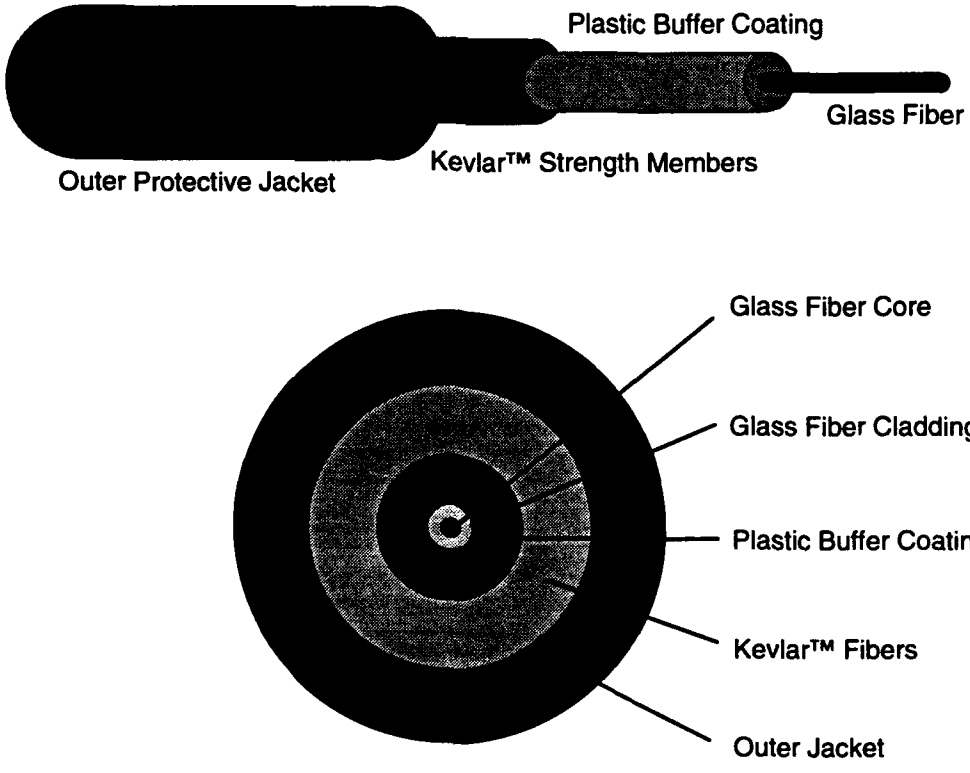


Figure 2-2
Fiber-Optic Cable

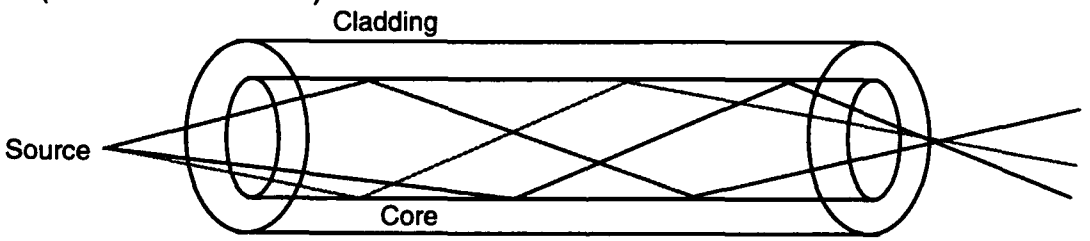
The construction of a typical interior distribution fiber cable (fig. 2-2) consists of the glass fiber (core and cladding) surrounded with a plastic buffer[11].

There are two primary types of optical fibers: single mode and multimode[12]. The differences between the two are primarily a question of how large is the core diameter. In singlemode fiber, the core diameter is only 7-9 microns thick (about 1/3000th of an inch). For multimode fiber, the core size ranges from 50-100 microns (1/500th to 1/250th of an inch).

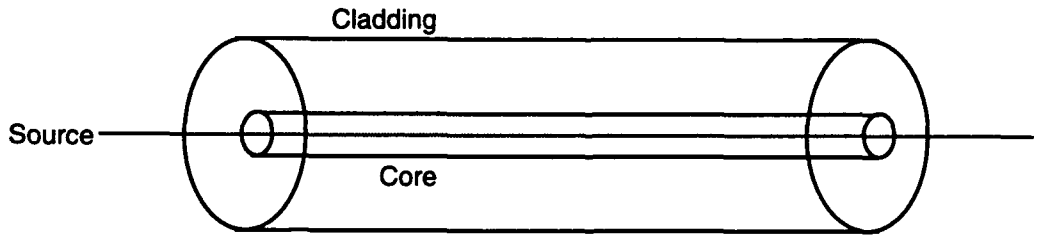
The concept here is the fact that in the "wider" (or "larger" core) multimode fiber, different rays of light bounce along the fiber at different angles as they travel through the core. Therefore, the light rays actually travel different total distances as they go from one end of a long fiber to the other end (fig. 2-3).

Since some of these light rays travel longer distances, and since the speed of light is a constant, some of the light will arrive at the end of the cable later than others. Therefore, when a signal pulse is put into one end, it may come out the other end exhibiting a little spreading or "dispersion". The longer the distance, the greater the dispersion. So, after awhile, the signal pulse will be so distorted it is no longer readable.

In single mode fibers, optical information is input into the glass as a single light ray, with no bouncing along the sides. So we have little or no dispersion even after very long distances (tens of kilometers).



a. Multimode



b. Single Mode

Figure 2-3
Comparison of multimode and single mode fiber

---

[11] This plastic buffer can be tightly formed around the glass - called a tight buffer, or there can be a gap between the buffer and the fiber(s) - called loose tube. Loose tube fiber cables are often filled with a water proof gel and multiple fibers.

[12] "The Fiber Optic LAN Handbook", Codenoll Technology Corp., 5th edition.

Since most of the distances here at NRaD are shorter than a few kilometers (within buildings or between buildings in a campus area) multimode fiber is the predominate choice for fiber distribution. Backbone links are either multimode or singlemode depending on length and bandwidth needs. However, as data bandwidth requirements increase over the same distances, more and more single mode fiber-optics may be needed.

Intrusion Detection Optical-Fiber Systems

Currently, there is only one NSA-approved, intrusion detection protected optical-fiber cable system for type I data, and that is the Hughes Intrusion Detection Optical Cable System (IDOCS). The McDonnell-Douglas Intrusion Detection Optical Communication System (MiDOCS)[13] is currently being evaluated by NSA, but is not yet approved. These systems work by continuously monitoring the fiber's condition for attempts to tap the fiber. If an attempt is detected, the transmitter/receivers on both ends will alarm and shut down until someone verifies that the cable hasn't been tampered with and then resets the units.

The advantage of these products over the Protected Distribution System (PDS) is that at distances of 100-200 feet, they start to compete in terms of cost, and, for distances beyond 500 feet they are far more practical. The advantages that they have over hardware encryption are that: 1) there is no encryption ignition key to have to load and manage, and, 2) there is no performance penalty; performance is at the full bandwidth of the network.

The disadvantages are, that like any system to protect data, they are very expensive[14], and they are more expensive to install.

Coaxial Cabling

Coaxial (coax) construction has a center core wire, surrounded by a dielectric insulator, then by a ground shield and finally, by an outer insulator jacket. Cables are rated by their diameter (the larger the diameter the less a signal is attenuated) and by their characteristic impedance's (or resistance). Typical cables used in networking are: RG-6; CAC-11; RG-59 for CCTV; CATV and broadband; RG-58 for thinwire ethernet; and RG-36 for thickwire.

The advantages of coaxial cabling are: high noise immunity, low cost, availability of products and a large knowledge base on installation and use. Disadvantages are: weight;

---

[13] IDOCS supports a full bandwidth ethernet at 10 Mbps, while MiDOCS supports full bandwidth FDDI at 100 Mbps.

[14] From $40K to well over $100K depending on the product and the amount of fiber cable purchased.

high attenuation, short relative distances compared to fiber, limited bandwidth, and a lack of new technologies being developed using coax.

Twisted-Pair Cable

There are two major types of twisted-pair cable. The first is shielded twisted-pair (STP), where there is a shield (foil) around the copper wire pairs that is grounded to one of the network devices that it's connected to. The second type is unshielded twisted-pair (UTP) cable (doesn't have any grounding shield).

Shielded twisted-pair cable is a good choice for high bandwidth (100-300 MHz), long distance (100-150m), low emissions (FCC B ratings), high RF noise environments. 10BaseT ethernet, 4-16 MHz Token Ring, and 100 Mbps FDDI over twisted-pair copper already have standards developed for distances up to 100m. The disadvantages of shielded twisted-pair cable are its higher costs relative to UTP, it's thicker and more rigid compared to UTP so it's more difficult to install, and its connectivity is more complex due to the grounding requirements.

Of the different types of UTP cable, the most commonly used are category 3, 4, and 5 type cables. The difference between the different types are the number of twists-per-foot in each pair and the relative difference of twists between the pairs. The twists in the pairs are used to attenuate signal coupling between wires. The different twists in the pairs are used to stop coupling from one pair to another.

Category 3 cable is called voice grade and is widely used by the telephone company. Because of the low number of twists-per-foot in a pair (4-5) this cable is highly susceptible to noise a higher bandwidth frequencies. Because of this, we want to discourage the use of existing telephone wire for networking. Appletalk and 10BaseT over short distances (<30 m) will work, but there might be problems.

Categories 4 and 5 are called data grade wire (they have much higher twists counts). Cat. 4 cable is certified for runs up to 100 m at frequencies to 20 MHz so it's acceptable for ethernet and token ring. Cat. 5 is certified to 100 MHz at 100m. It would be acceptable for FDDI except that FDDI has a clock rate of 125 MHz. The standards bodies for fast ethernet and FDDI are working towards a UTP standard.

Wireless

Over the next few years wireless communications technologies will become a major issue that this station will have to handle. One technology that is being used today are one-way messaging systems (pagers). Some pagers handle alphanumeric data and are even integrated with E-Mail systems. Other technologies are RF, spread-spectrum RF, microwave, and infrared.

Problems with these technologies are as follows: lack of distance; problems with barriers (walls, buildings, etc.); purchase costs are high; possible licensing requirements by the FCC for RF technologies; problems with interference and noise; limited bandwidth, and, except for spread-spectrum, an inherent lack of security.[15]

Spread-spectrum networks have a certain amount of security built in because the bandwidth being used is split and distributed over multiple, non-contiguous frequency bands (some network devices even have an automatic channel-hopping capability). So, unless a person, who is trying to "tap" a network session, knows ahead of time what frequencies are going to be used, the odds against finding and re-assembling the data stream in the correct order to listen to a transmission are astronomical. However, even though this technology was originally developed for military use, no Commercial Off-the-Shelf (COTS) spread-spectrum data network devices have been approved for the transmission of Level I or II data. Nevertheless, we recommend that this technology be considered whenever wireless network communication is needed for Level II data at NRaD.

Advantages are mobility and you don't need to wire (or re-wire when the office changes). With the future sales of personnel data assistants (PDA's - hand-held computers), connections to pager, to cellular and to LAN-based wireless networks will become in greater demand.

Other Factors

Physical environment must be considered to prevent signal degradation over the physical media.

- Damp or moist environments can cause signal grounding at cable connectors and coupling adapters. Shrink tubing or conferral coatings are an effective method to ensure waterproofing.

---

[15] Unless wireless transmissions are encrypted, anyone within range of the transmitter can pickup and read the information being sent if they have the right equipment.

- External RF noise might be a significant problem regarding signal distortion and deterioration of communications over copper cable. It is important to use high quality materials and cables (dielectric and jacketed or armored shielding) to minimize or eliminate induced noise onto the wire. It is best to provide maximum spacing between a wire cable link and noise sources. For full noise and isolation protection, fiber-optic cable is the preferred medium.
- As a precaution against lightning, buried or aerial cable routing must avoid the highest points of the local terrain. Always consult a certified Civil and Electrical Engineer for design issues pertaining to safety, mechanical and electrical codes.
- Maintain environmental conditions to manufacture's recommended conditions (i.e., temperature and humidity) to prolong material life.

2.2.3 Other Devices and Components

Along with the physical media, there are three other types of devices that make up the physical plant for a network. These devices can be classified as being either passive (not using any power), active (needing power to operate) or support equipment. With the exception of some types of gateways (to be described later) these items typically fall in the first three layers of the ISO Reference Model.

ISO Reference Model

No discussion of networking is complete without a section about the International Standards Organization (ISO) Reference Model for Open Systems Interconnection (OSI)[16]. Sometimes referred to as the OSI seven-layer protocol stack (fig. 2-4), the reference model is useful in describing "like" network functions. By standardizing the interfaces between these architectural layers, it is possible to substitute new technologies at any layer without having to change hardware or software at other layers (that's the theory, and most of the time it works - anyway, it's a good goal).

[16] Data Communications, Computer Networks and OSI, 2nd ed., Addison-Wesley Publishing Company, Fred Halsall.

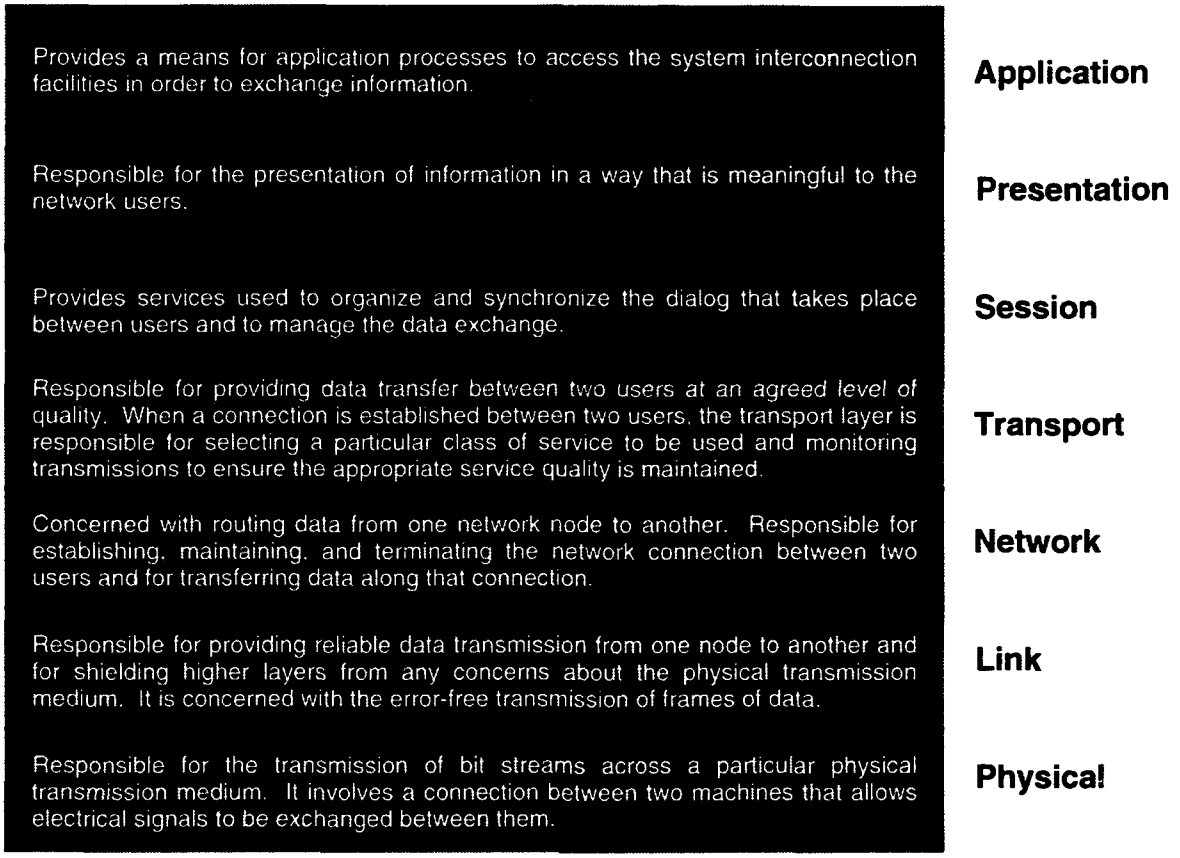


Figure 2-4
ISO reference model

Passive Devices

Connectors, distribution taps, attenuators, transceiver taps and passive filters are examples of passive devices. These devices all allow connection to the physical media, join physical media segments together, or modify the signal coming from the media.

Our recommendation is that standards based connectors be used whenever possible. For instance, "ST" fiber connectors; FDDI "MIC" connectors; ethernet "BNC", "AUI", and 10BaseT RJ45 connectors; and DB-9 or DB-25 connectors for serial applications, are examples of connectors that have been standardized as far as their physical characteristics. However, in the case of serial connections, signaling levels and wire usage have common configurations, but the standards are often not specific enough to insure communications just by plugging two connectors together. Often times, getting two devices talking to each other still takes staring at data sheets and fiddling with a breakout box in order to figure out what pins in a connector need to be reconfigured.

Two issues about passive devices need to be explored in regards to security. The first concerns the physical protection of connectors and taps. The second relates to the reliability of the connections.

With regard to the physical protection of passive devices, remember, that a signal passes through these devices between two lengths of the same media, or from the media to an active device, without the data being processed in any way. Because of this, it is usually not possible to detect when someone has unknowingly added a new connection, without visual inspection or without using a mechanical device to detect a change.

Visual inspection is tracing a cable, looking at a patch panel, or looking at a tap location to see if anything has changed or been added.

An example of a mechanical inspection device is a power meter. By comparing the strength of the signal levels (electrical or optical) at a connector to a baseline measurement, it can be determined if a link has been degraded. Once a discrepancy has been determined, the reason for the degradation needs to be resolved, such as, is there a short or open in the line, has the physical properties of a connector changed (corroded pins, dirty fiber), or has someone tapped into the line?

Another type of mechanical measurement device is a time domain reflectometer (TDR for copper wire, or OTDR for fiber). These devices characterize the physical properties of the media: length and attenuation locations, such as, splices, in-line connectors, kinks, and micro-bends and may have the capability to store this information on a printout or computer file. Again, by comparing periodic measurements to a baseline, it is possible to discover when changes have been made; however, no matter what method is used, good configuration management and record keeping is necessary to track changes from a baseline.

The second security issue is to insure good reliability of the passive devices. This is important to maintain a high quality of service. Poor workmanship or low quality materials can lead to intermittent or total failure of a connection. These failures can be very disruptive to a network, and failures that just add noise to a network can be very difficult to locate. Our recommendation is that all physical installations or connections be tested and inspected for adherence to specification before being accepted into service.

We also recommend that passive tap networks, such as thick and thin wire ethernet and broadband CATV networks should avoided, or should be phased out, for the transmission of classified or sensitive data unless the segment is physically protected. This recommendation is made due to the difficulty in keeping these segments under configuration control (connections are often made in a hurry and the documentation is forgotten). Also, it is very easy to tap onto the network and it can be very difficult to

discover these connections. Isolation of problems on the net without bringing down a significant portion of a segment is also a major concern. Of course, any type of media can be tapped and only data that has been properly encrypted is safe. So, other criteria (such as, reliability and cost) need to be considered before making a decision.

Active Devices

Some examples of active devices are amplifiers, repeaters, transceivers, media access units (MAUs), multiplexers, modems, network interface cards (NICs), network interface units, bridges, routers, gateways and hub/concentrators. There are three classes of active devices that we must be concerned with: The first class are distribution devices that connect or extend multiple network segments or devices together without any processing the data packet's addresses; the second type are "inter-" or "intra-" networking devices that connect to two or more LAN(s) or WAN(s) and will make decisions on how data is to be directed based on address information; and the third type of devices consist of the hardware needed to connect individual nodes (e.g., computer) to these network segments.

Distribution Devices

Distribution devices (amplifiers, repeaters, multiplexers, hub/concentrators) are devices that typically re-time or strengthen a signal in order to extend the range of a network. For instance, an ethernet repeater allows an ethernet segment to be extended beyond the distance limitation for the media being used (for example; from 500 m, for a thickwire segment, to 1000 m, with two thickwire segments connected with a repeater).

Until recently, most of these devices where "dumb" in that they did not collect and store any data about their performance and the condition of the network. Typically, the information that was supplied was through LEDs that indicated usage and error conditions on the net by lighting up or flashing. Now, many devices have management capabilities built-in, such as the Simple Network Management Protocol (SNMP), and some hub devices have had additional management control capabilities included such as network data collection and security features that are accessible through the network or through an "out-of-band" link via a console port for TTY or modem connection. It is important that the management function of the devices be password protected and settings be documented. If the console port is not password protected, the unit should be physically isolated from casual access.

Some hubs have a DES encryption capability or have a feature whereby data is sent down only on the cable that is connected to the target machine. The other machines see only scrambled data or a jamming signal. While these features are not sufficient to protect level I data, they should be evaluated as possible methods to protect level II data from disclosure.

While these methods may not prevent a sustained, determined "inside" attack, they will prevent most curious or disgruntled users from putting their network interface into a "promiscuous" listening mode and collecting data. Most LAN technologies work by having the connected devices share the available bandwidth. This is done by the hardware having the capability to send or receive all data packets. It is usually only the hardware driver software that controls whether or not a node actually processes the data that it receives. If the standards-based software drivers are substituted with software that will record all data or will look for particular packets (username/password combinations, for instance) then the user of that machine has the potential for compromising the system.

This type of software is becoming more and more available. Possible sources are underground bulletin boards for "break-in" versions, and legitimate channels, such as, network equipment vendors selling network monitoring software that can turn your PC into a network protocol analyzer and monitoring station. Discovering the presence of this software is impossible, so it is important that the risk of disclosure of data be evaluated against the cost of protecting the network.

The main thing to remember is that you need to be aware of, the importance of the data that will be used on your machine. If it is sensitive information that must not be compromised, then contact your DADPSSO. They can get help in evaluating what protection methods will best protect your data from the ADP security group.

Addresses

There are two types of network addresses for nodes or groups of nodes connected to a network: 1) A physical address that is often hard coded onto the network interface and operates at the link layer; 2) A protocol address that works at the network layer and is dependent on the protocol being used (e.g. ISO/OSI, TCP/IP, Novell, DECnet, etc.). Addresses that are set aside for groups are called either broadcast addresses (all nodes) or multicast addresses (predefined group or population).

Addresses are used to identify a node in the network. They are necessary for sending nodes and Inter-networking nodes to know how to direct data packets, and for receiving nodes to know when a packet is intended for it. For most protocols, both the source and destination addresses are included within the data packet.

Protocol addresses typically have two parts, a network portion that identifies a net or subnet group, and a node address that specifically identifies a machine.

2.2.4 Inter-networking Equipment

"Inter-" or "intra-" networking equipment are devices such as bridges, routers and gateways (fig. 2-5). The devices described above, work at the physical layer of the ISO reference model. These Inter-networking devices work at the link layer for bridges, the network layer for routers, and depending on the function being performed, a gateway can work from the network layer up to the application layer.

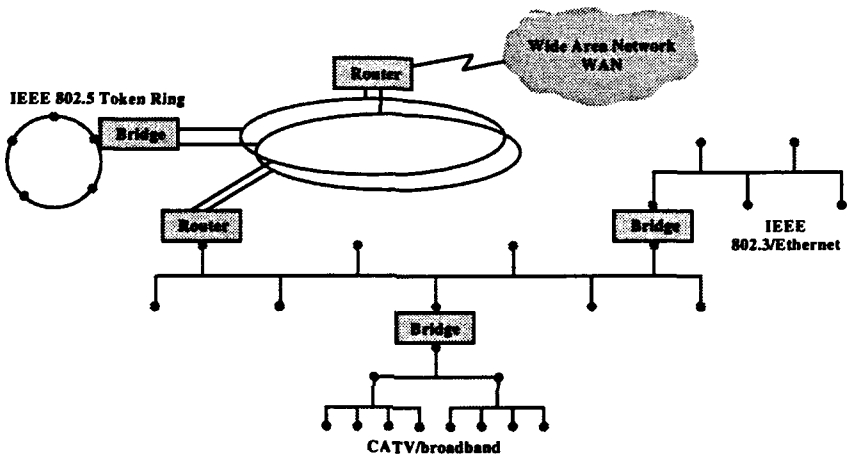


Figure 2-5
Inter-networking

Bridge

A bridge works by connecting two networks or network segments of like or dislike media types together. They operate by remembering the port at which an address has been previously seen. When a data packet that is bound to another node is received by a bridge (filtering), it will look at a lookup table to determine if the target node is on the same side of the network as the source machine, in which case it will do nothing. If the packet is located on a different network, connected off of a different port, it will "forward" the packet to that network. If the bridge has never seen an address before, since the last time the bridges lookup table was flushed, or if the packet is a broadcast or multicast, the packet will be sent out through all of the ports. The bridge tables will be updated when it sees a packet that has been generated by a machine. Bridges are useful in isolating data packets from one network that is not intended for a machine located on another, so they are used to decrease the load between segments. They typically do not

evaluate what type of protocol or data type is being transferred, so they make poor security firewalls.

Routers

Routers work at the network layer by evaluating the protocol net/subnet address and the protocol type of a data packet. It is the capability to look into the packet and evaluate more thoroughly what type of packet is being sent as well as the node and net/subnet. This allows the network administrator to setup firewalls to exclude traffic from certain nodes, net/subnets or packet types. For instance, you may want to block all packets requesting remote logins, or all file transfers from networks outside of NRaD. For more information about the security capabilities of routers, see your DADPSSO. They will get you touch with one of the station's network experts.

Gateways

Gateways work by translating between different protocols or applications. For instance, you may have an application that needs to communicate between two different machines that use two different protocols (TCP/IP and DECnet as examples). A gateway will need to be setup to re-format and resolve addressing differences between the two different packet types. Because of the large number of combinations that are possible between applications and protocols, gateways typically have to be created for that specific purpose.

Another type of gateway is an application translator such as an email gateway. One possible function of this type of gateway would be to filter email messages that have been labeled with different classification levels (note: that general-purpose, multi-level security email gateways do not exist at this moment), or as a email format translator (e.g., SMTP to Novell MHS or ccMail). Note that sometimes routers are referred to as gateways.

Protocols

(this section will be added during a later revision of this document)

Support Equipment

Examples of support equipment are communications closets, equipment racks, patch panels, power supplies, conduit, wire trays and air conditioning. While this equipment is

not directly responsible for transmission of data over a network, they are important in protecting equipment and cables, supplying reliable power, and organizing equipment to keep things neat and tidy.

Communications closets and areas should have limited access and be locked when not occupied, even for non-sensitive/classified data networks. Again, this may or may not keep a determined person from gaining access to this equipment, but it will more than likely thwart the just curious and clumsy.

For devices in an open storage classified space, equipment should be placed out of the way or in equipment racks. Equipme racks or enclosures in non-secure or occupied spaces should be locked.

Cables should be neatly routed, to improve traceability of problems, and unused cable should be removed. It is also a good idea to protect long runs of fiber optic cable in conduit or innerduct whenever possible. This is due mostly to help identify the cables as fiber optic. Most fiber-optic cable construction is robust enough to protect the enclosed optical fibers from routine to even moderately rough handling. However, snagging a cable and dragging it may cause stress at the termination points and splices and connectors can be damaged.

We recommend that all electrical equipment be connected to surge/power protection of some type to keep power spikes from frying electronics. Uninterruptable Power Supplies (UPS) for network devices are a good idea for networks that require high availability, especially for networks that have nodes that are powered by UPS connected to them.

Good housekeeping practices are a must for good security. Configurations can be documented and verified far more easily, and problems can identified and corrected quicker. Also, it may keep your boss happy when a VIP walks through an area and comments on how professional things look.

2.3 Security Issues

Multi-Level Security (MLS)

MLS systems and MLS networks are on the threshold of commercial development and production. A few have been approved on NSA's Evaluated Products List. Like all systems and networks, a commercial product, such as MLS systems and networks, must

be implemented with a security policy and design in mind that encompass an operational environment compliant with Navy minimum security safeguards. The accreditation authority for MLS is beyond CO, NRaD. Because MLS systems or networks are "trusted" to ensure compliance with security policy, extra attention in system/network administration must be provided by management for functions; such as, configuration management, access control, audit of system usage, and documenting the security policy and procedures for the system.

Protected Distribution Systems (PDS)

PDS's are an effective means to protect classified data transmitted on communications media traversing through unsecured areas. PDS's require strict physical and TEMPEST design approval, configuration management approval, and physical controls requisite for the highest classification to be transmitted through the PDS. PDS's can be costly to design, build, manage and maintain.

Encryption Devices

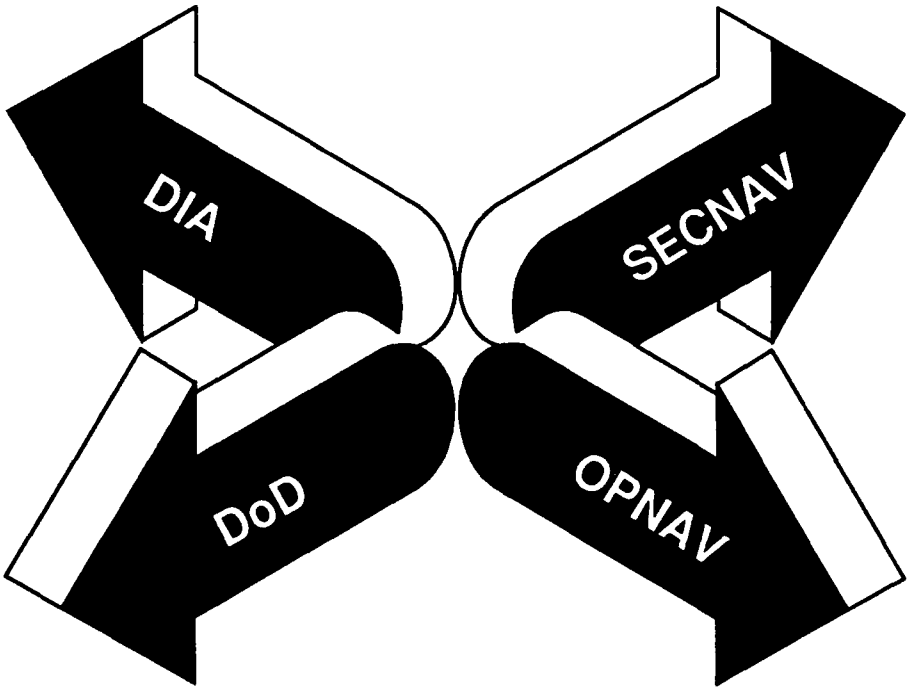
Encryption (scrambling) is an effective means to transmit sensitive or classified information through unsecured areas over dedicated or commercial communications links, to a destination secured at the same classification level as the source. Many Navy-approved encryption devices exist, and these devices are strictly controlled and regularly inventoried under the NRaD CMS custodian (or STU-III Manager for STU-III phones and secure data devices).

TEMPEST

TEMPEST is a short name for the Navy program to control compromising emanations. TEMPEST issues traverse across not only physical properties of electronic equipment that process classified information, but also traverses across the management and system user levels, for the day-to-day operation and configuration control. Outside of approved TEMPEST enclosures, a strict regime of configuration management and user procedures must be closely followed.

CHAPTER 3

POLICIES AND PROCEDURES



CHAPTER 3

Security Guidelines for Compliance with NRaD Networking Policies

3.1 Purpose

This chapter establishes the security guidelines that support NRaD networking policies. It is intended for reading by DADPSSOs, ADPSOs, Network Managers, System Managers, and any other persons or groups wishing to establish network connections a. or with NRaD. These guidelines are applicable to any information handling machine that connects to any communication resource within NRaD and the users of these machines. As addressed in Section 1.3, when these guidelines cannot be met, early consultation with the DADPSSO, NSO, NSM and ADPSO should resolve the issues in a manner that optimizes the balance between controls placed on the network and the total costs of such controls.

3.2 Security Policies for All NRaD AIS & Networks

All Automated Information Systems (AIS's) networks and computer resources will be protected by the continuous application of appropriate protective measures. These security measures are relevant to operation of networking at NRaD, however, additional security policies may be required for connectivity and operation off-Center.

3.2.1 Accreditation

Automated Information Systems (AIS's), networks, and computer resources must be accredited by the appropriate Designated Approval Authority (DAA) based on a documentation, certification, and risk management process. Accreditation is a formal declaration by management that authorization for operation of a specific application of AIS, network, or computer resource meets prescribed security requirements.

AIS's and networks not accredited may operate if the appropriate DAA (defined in OPNAVINST 5239.1A) has issued an Interim Authority To Operate (IATO) for a period not to exceed one (1) year.

An accreditation or IATO may be issued for an entire system or group of systems in those instances where the DAA has determined that such a "blanket" IATO or

accreditation represents the most efficient means of maintaining system operability while ensuring security

Accreditation's will be reviewed at least once every three (3) years; or when changes to the functionality, architecture, data processed, user population, or environment might result in increased exposure of the AIS, network, or computer resource to harm. If no such change has taken place, the accreditation may be reissued based upon a thorough review of the previous accreditation documentation.

Accreditation of embedded computer systems is the responsibility of the associated DAA.

- Navy program sponsors and Marine Corps program managers will require that developing agencies ensure that systems are certified, and the end users and DAA's are provided with standard operating procedures and documentation to permit accreditation with minimal effort by end user commands.

- Upper echelons of a chain-of-command may elect to group accredit specific systems under their operational control to relieve subordinate end users of this administrative burden. With the concurrence of the concerned Officer's of Primary Responsibility (OPR's), senior commanders may issue an accreditation covering the entire population of a given system. Accreditation in this case applies to systems such as process control applications that cannot be modified by the end user except by extraordinary means.

Figures 3-1 and 3-2 provide steps and required documentation for requesting an accreditation for NRaD network resources. Additional forms and Network Administrators tools may be found in Appendix D of this document.

Figure 3-1

How to Request Network Accreditation

1. The NRaD Network manager has been formally identified and appointed in writing.

2. If NRaD is designated as Central Design Agent (CDA) or Network management by higher authority (i.e., Project Manager at Headquarters) this must be done by written appointment.

3. A Network Security Officer (NSO) is appointed in writing, and approved by Commanding Officer, NRaD. The appointment memo must be addressed to Commanding Officer NRaD, via the ADPSO. NSO's duties are identified in Chapter 2 of OPNAVINST 5239.1A, Chapter 13 of NOSCINST 5500.1A, and this document.

4. Network management must first, based upon the planned network community, decide what the highest classification or data sensitivity will be handled, transmitted, or stored on the network and all components.

5. Network management and the NSO must coordinate the network security design requirements, so that they are in compliance with the Navy AIS security program.

6. Network management must, in advance, give consideration to network design and installation. Design and installation approval for a TEMPEST Protected Distribution System (PDS) must be obtained prior to installation of the PDS. Management must give consideration about PDS's, to include the following: design, installation, physical protection, personnel clearances, and required cryptographic equipment and material to support data transmissions at the highest classification.

7. Management must consider where classified open storage areas (i.e., strongrooms) will be required, and, if necessary, take steps to build and obtain certification for a classified Open Storage area where classified material, equipment and network components openly contain classified information.

8. Because of the shared nature of networks, network management must give consideration to the extent of required auditing on the network controller and all network host systems, the type of access controls for network and host systems, configuration management, and consideration about all physical and environmental controls to be implemented.

- Network management must ensure the development of accurate and up-to-date diagrams of network connectivity that reflect full network topology and logical connectivity, as part of network configuration management.
- Each remote host system on the network must have a formally appointed Terminal Area Security Officer (TASO) at the host site. The TASO must be appointed in writing by host site management, and a copy of the appointment letter submitted, and maintained by, the NSO.

- Network management or the NSO, or both, must develop a tailored Network Security Policy and Plans Handbook (NETSPPH) for the network's operational environment (as identified by a formal network security design by network management). The NETSPPH must be usable by all network personnel, to include: network management, network maintenance personnel, host system management, host system users, and security personnel. The tailored NETSPPH ensures uniform understanding and compliance with specific required network security policy, at all levels on the network.
- A formal Memorandum of Agreement (MOA) must be developed and signed between Commanding Officer (CO), NRaD and the senior officials from remote host sites (non-NRaD, such as another Navy activity, government agency, or contractor sites) directly linked to the NRaD network. For interconnection of NRaD systems belonging to, and located in, areas under other NRaD management, other than network management, then an MOA must be signed between network management and management from the host site. For each MOA submitted, a copy of the remote host system's current AIS accreditation letter must be affixed to the MOA, to show required security safeguards are present and are approved for operation.
- Network management or NSO, or both, must ensure that for each remote host system or remote interconnected network that requires direct connection with an NRaD network resource, the remote host system or network must have a current security accreditation (by its' local Designated Approval Authority (DAA), prior to being granted physical connectivity to the NRaD network resource.
- For multiple service/agency network connectivity, the entire network accreditation must be done jointly, based upon prior accreditation of each network host system.
- Network management must ensure each physical location where the network components and cables reside or traverse through, that the entire network is properly protected at all times for the highest data classification or data sensitivity that is resident, transmitted, or handled on the network. At remote host system sites that have a strongroom, a copy of the local DAA's letter of approval for the Strongroom, will be provided to network management.
- To use a coined phrase:

  "A network is only as strong as it's weakest link!"

Figure 3-2
AIS Accreditation Documentation Requirements

DOCUMENTATION	CLASSIFIED	SENSITIVE UNCLASSIFIED	UNCLASSIFIED
SYSTEM ID FORM	YES	YES	YES
ENVIRONMENTAL AND PHYSICAL SURVEY	YES	YES	NO*
SECURITY OPERATING PROCEDURES (SEE NOTE 1)	YES	NO*	NO*
TVAR REQUEST	TS ONLY	NO	NO
CONNECTIVITY/COMMUNICATIONS DIAGRAM (SEE NOTE 2)	YES	NO*	NO*
OPEN STORAGE CERTIFICATION (SEE NOTE 3)	YES	NO	NO
RISK ASSESSMENT (SEE NOTE 4)	YES	YES	NO*
CONTINGENCY PLAN (SEE NOTE 5)	YES	YES	NO*
ST&E PLAN TEST	YES	NO	NO

(3/93)

* For multi-user systems (Host) this document may be required as shown. Contact Electronic Systems Security Group for guidance.

Note #1: Security Operating Procedures (SOP) are required for system unique or complex operational environments not covered by the Security Policies and Procedures Handbook (SPPH).

Note #2: Diagram should show physical layout of all system equipment, all cable runs to computers, electronic devices (telephone and communication) and network interfaces (internal and external).

Note #3: Request written Certification for Open Storage of classified information and material from the Information, Personnel, and Operations Security Group.

Note #4: The Information, Personnel, and Operations Security Group will provide guidance for complex systems. For other than complex systems, a SIF combined with Environmental & Physical Survey will suffice.

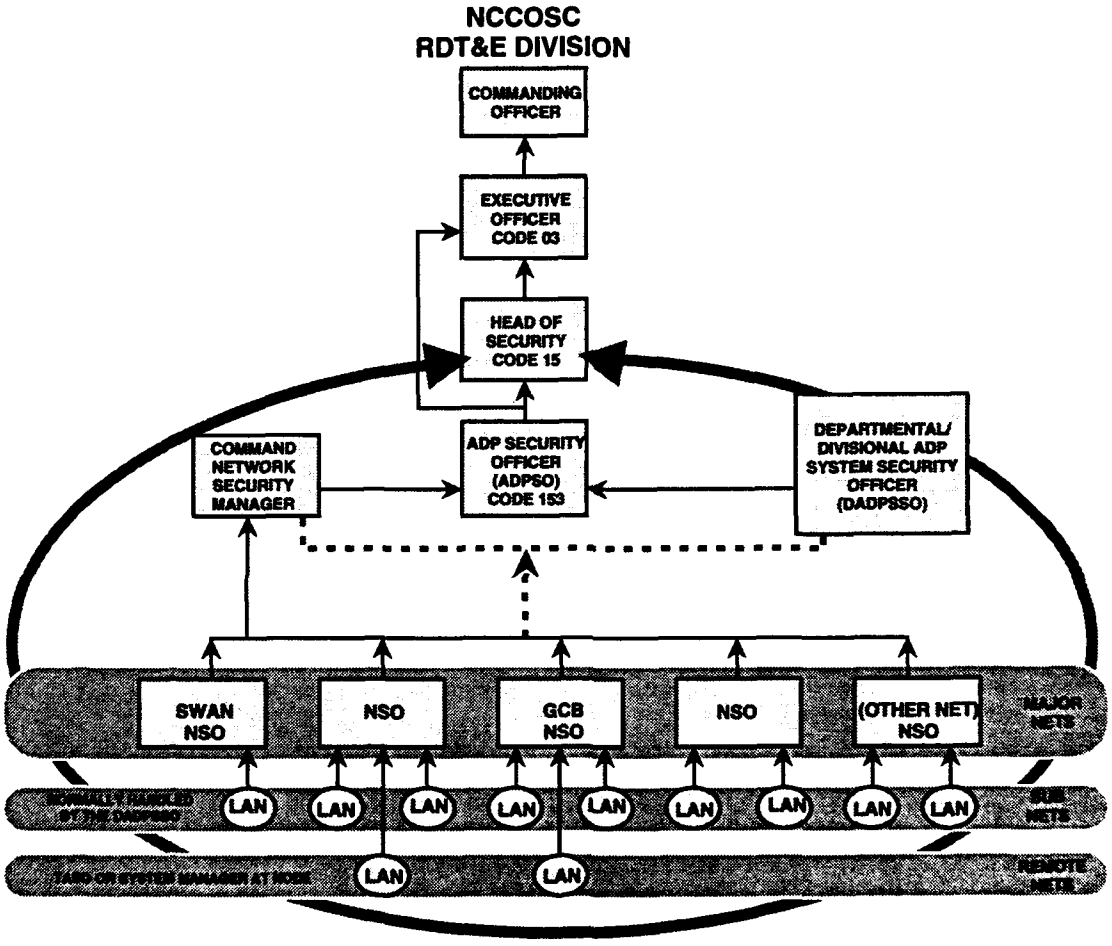
Note #5: Information Systems Council (ISC) must authorize contingency plan development/implementation based upon written justification via NRaD ADPSO.

3.2.2 Security Personnel Roles

Figure 3.3 details the network security roles for NRaD.

Figure 3-3

NETWORK SECURITY RESPONSIBILITIES



3.2.2.1 Designated Approving Authority (DAA)

The official who has the authority (i.e., DAA's are identified by OPNAVINST 5239.1A) to decide that an AIS, network, or computer resource may operate based on an acceptable level of risk considering the operational need for, and threats to, the system and is responsible for issuing an accreditation statement that records the decision. See Figures 3-4 and 3-5 for a listing of DoN Network DAA's.

3.2.2.2 ADP Security Officer (ADPSO)

The ADPSO reports to CO, NRaD, and implements the overall security program approved by the DAA. The ADPSO focuses on AIS security. The ADPSO should not participate in the day-to-day operation of the AIS.

Specific security responsibilities are:

- Ensure that the AIS security program requirements are met, including defining the security mode, specific security requirements, protocols, and standards. Develop applicable AIS security procedures.
- Implement the risk management program defined by the Department of Navy (DoN). Verify that the risk assessment is performed and that threats and vulnerabilities are reviewed to evaluate risks properly.
- Verify that appropriate security tests are conducted and that the results are documented .
- Review the accreditation plan and the re-accreditation activities; develop a schedule for the re-accreditation tasks; initiate recertification and re-accreditation tasks under the direction of the DAA.
- Assist in site-configuration management by reviewing proposed system changes and by reviewing implemented system modifications for adverse security impact.
- Ensure that AIS security is included in all the contingency plans.
- Provide the DAA with the certification package to show that the AIS satisfies the security specifications for the data it processes, stores, or transmits. Document and maintain the evidence contained in the certification package.
- Monitor AIS personnel security procedures to ensure that they are being followed; coordinate and monitor the initial, and follow-up, security training for AIS personnel.
- Maintain a current AIS security plan.
- Ensure Terminal Area Security Officers (TASOs) are appointed, in writing, for remote sites connected with NRaD AIS resources.

Figure 3-4

**Navy Designated Approving Authority (DAA)
For ADP Networks Processing Level I
(Classified) Data**

TYPE OF DATA PROCESSED	SECURITY MODE OF OPERATION	DAA	DON POC
NATIONAL CRYPTOLOGIC	ALL	NSA/CSS	COMNAVSECGRU
SCI	ALL	DNI/DIA	SPAWAR CSM
SIOP-ESI	DEDICATED	CNO	SPAWAR CSM
TOP SECRET	MULTILEVEL	SPAWAR CSM	SPAWAR CSM
	CONTROLLED	SPAWAR CSM	SPAWAR CSM
	SYSTEM HIGH	CO	ADPSO
	DEDICATED	CO	ADPSO
SECRET	MULTILEVEL	SPAWAR CSM	SPAWAR CSM
	CONTROLLED	SPAWAR CSM	SPAWAR CSM
	SYSTEM HIGH	CO	ADPSO
	DEDICATED	CO	ADPSO
CONFIDENTIAL	MULTILEVEL	SPAWAR CSM	SPAWAR CSM
	CONTROLLED	SPAWAR CSM	SPAWAR CSM
	SYSTEM HIGH	CO	ADPSO
	DEDICATED	CO	ADPSO

Figure 3-5

**Navy Designated Approving Authority (DAA)
For ADP Systems or Networks Processing Level II
(Sensitive Unclassified) Data**

TYPE OF DATA PROCESSED	SECURITY MODE OF OPERATION	DAA	DON POC
PERSONAL	LIMITED ACCESS	CO	CNO (OP-09B)
FOR OFFICIAL USE ONLY	LIMITED ACCESS	CO	CNO (OP-09B)
FINANCIAL	LIMITED ACCESS	CO	NAVCOMPT

3.2.2.3 Network Security Manager (NSM)

The NSM is responsible for the overall security operation of networks at the Center and is the focal point for policy, guidance, and assistance in network security matters. In addition, the NSM ensures that the network complies with the requirements for interconnecting to external systems. The NSM coordinates with the ADPSO and does not participate in the day-to-day operation of the network. The tasks of the NSM are comparable to those of the ADPSO. For ease of comparison, the security responsibilities are listed in the same order as those for the ADPSO.

- Ensure that an Network Security Officer (NSO) is appointed for each network.
- Ensure that the AIS security program requirements are met, including defining the security mode, specific security requirements, protocols, and standards. Develop applicable network security procedures.
- Implement the risk management program defined by the DoN. Verify that the risk assessment is performed and that threats and vulnerabilities are reviewed to evaluate risks properly.
- Verify that appropriate security tests are conducted and that the results are documented .
- Review the accreditation plan and the re-accreditation activities, develop a schedule for the re-accreditation tasks, and initiate recertification and re-accreditation tasks under the direction of the DAA.
- Assist in-site configuration management by reviewing proposed system changes and reviewing implemented system modifications for adverse system impact.
- Ensure that network security is included in all the contingency plans.
- Provide the DAA with the certification package to verify that the network satisfies the security specifications for the data it processes, stores, or transmits. Document and maintain the evidence contained in the certification package.
- Provide the DAA with written certification that the network satisfies the security specifications for the data it processes, stores, or transmits. Ensure that the documentation to support the certification is developed and maintained.
- Monitor implementation of AIS personnel security to ensure that AIS procedures are being followed; coordinate and monitor the initial, and follow-up, security training for AIS personnel.
- Maintain a current AIS security plan.

- Manage routing control for security within the network; specify links or subnetworks that are considered to be trusted based on specific criteria.
- Manage network addressing conventions for all Center networks.
- Investigate security incidents on Command networks.

3.2.2.4 Dep't/Division ADP System Security Officer (DADPSSO)

The DADPSSO reports to the ADPSO to ensure compliance with AIS security procedures for cognizant AIS and networks. Depending on the size and complexity of the AIS, the DADPSSO also may function as the NSO. The duties of the DADPSSO are as follows:

- The DADPSSO will be involved in all phases of cognizant (intra) departmental/divisional network processes from initial design, through installation, certification, operation, maintenance, and final approval. When a DADPSSO has not been appointed for intra-Departmental networking, then a NSO will be assigned.
- The objective of the DADPSSO position is to support security and accountability policies throughout an AIS or networking operation or both. To accomplish this goal, two key requirements are: 1) the separation between Administrator and Operator functions, and, 2) between relevant security and non-security functions of System Administrators. The duties of the DADPSSO are listed in Figure 3-5.

3.2.2.5 Network Security Officer (NSO)

The NSO implements the network security program and acts as the point of contact for all cognizant network security matters for major networks as determined by the ADPSO, NSM, and DADPSSO. The responsibilities of the NSO are similar to those of the DADPSSO, with the NSO concentrating on network security, and the DADPSSO concentrating on AIS security. NSO's will report to the NSM/ADPSO and the NSO shall have the same responsibilities as the DADPSSO for interdepartmental and interagency matters (contractor access, etc.). The NSO and DADPSSO will coordinate efforts to provide overall network security. The NSO will have ultimate authority regarding cognizant network security related matters.

An NSO for a major NRaD network must be involved with day-to-day operation and administration of the network. The NSO ensures that the network managers security

policies, and DoN's minimum security policies, are documented for use by users at each host system and node site connected to the network. The NSO ensures security safeguards are appropriately implemented on the network by periodic application of the Navy Risk Management Program, by regular security auditing, and monitoring with security-check software tools.

The security responsibilities of the NSO are as follows:

- Obtain written approval from the DAA to process classified or sensitive unclassified information on the network.
- Maintain the security processing specifications for the network.
- Ensure that standard security procedures and measures that support the security of the entire network are developed and implemented. Conduct periodic reviews to ensure compliance with network security procedures.
- Ensure that network security is included in all the contingency plans and that the contingency plans are tested.
- Maintain the site-specific portion of the accreditation documentation.
- Ensure that physical measures to protect the facility are in effect and that measures to protect mission-essential, sensitive data processing activities are implemented. Maintain liaison with organizations that are responsible for physical security (e.g., military police, fire control officials, base power plant officials, and emergency services).
- Review network configuration changes and network computer changes (or modifications) to ensure that network security is not degraded (including interfaces to separately accredited AIS's). Ensure that network components (i.e., hardware, software, and firmware) are included in the configuration management program.
- Select security events that are to be audited or remotely collected; establish procedures for collecting the audit information; review audit reports.
- Ensure that host system management verifies security clearances and access approval for personnel using the network.
- Coordinate and monitor initial and periodic security training for network personnel. Verify that all users receive network security training before being granted access to the network.
- Provide users with plans, instructions, guidance, and standard operating procedures regarding network operations. Conduct periodic reviews to ensure compliance.

- Verify that personnel security procedures applicable to the operation of the computer facility are followed.
- Report physical, personnel, and AIS security violations to the ADPSO/NSM. Report system failures that could lead to unauthorized disclosure.
- Review reported security problems and inform the NSM of security difficulties. Ensure that Terminal Area Security Officers (TASO's) evaluate, document, and report security problems or vulnerabilities at their respective sites.
- Based upon degree-of-risk for compromise of information, the NSO will perform partial or complete suspension of network operations, if any incident is detected that may affect security of the operation.
- Monitor the system recovery processes to assure that security features are correctly restored.
- Maintain guidelines that ensure that the physical, administrative, and personnel security procedures are followed.

3.2.2.6 Terminal Area Security Officer (TASO)

The TASO reports to the DADPSSO and is responsible for security procedures in an assigned remote terminal area. System access from the TASO's assigned remote terminals will not be allowed without authorization from the cognizant security officer.

The TASO has the following security responsibilities:

- Ensure that there are written instructions specifying security requirements and operational procedures for each terminal area.
- Ensure access to a terminal is only to users with the need-to-know, clearance, and access approval for data that may be accessed from that terminal.
- Perform an initial evaluation of security problems in the assigned terminal area(s) and notify the DADPSSO of all security violations and practices that may compromise system security.
- Verify that the physical security controls are in place and operational, for example, physically protecting the network interfaces (hardware connections).
- Collect and review selected remote facility audit records; document any reported problems; and forward them to the DADPSSO.
- Participate in security training and awareness.
- Ensure that the equipment custodian has all the component serial numbers written down and stored in a secure place.

3.2.2.7 Security Responsibilities of Other Site Personnel

Because the overall security of a site is subject to the cooperation of everyone involved in the system, the discussion of roles and responsibilities would not be complete without mentioning the system manager and the users. Everyone is responsible for knowing the security procedures and mechanisms that are in effect for a particular system, for following all procedures applicable to security, and for reporting potential security incidents. In addition, specific responsibilities for other individuals are listed below.

The system manager will:

- Coordinate with the DADPSSO on information security requirements and with the NSO for network security requirements.
- Establish or confirm the overall security classification of the applicable resources and establish restrictions, or special conditions, for the use of the data.
- Periodically review the data to verify that the security classification or sensitivity is correct.
- Authorize individual or group access to specific resources.
- Participate in the development of a formal need-to-know policy.

The users will:

- Use the system only for authorized purposes in accordance with security procedures and guidelines.
- Maintain individual accountability (e.g., do not share passwords).
- Protect classified and other sensitive material.

3.2.3 Life-Cycle Management

To ensure compliance with security policies, action shall be taken throughout the life cycle of an AIS, network or other computer resource.

The developing activity is responsible for ensuring the early and continuous involvement of the users, security staff, data owners, and DAA's in defining and implementing security requirements of the system.

Acquisition and procurement documents for all Department of the Navy AIS's, networks, or other computer resources must require compliance with this and related computer security directives.

To the maximum extent possible, computer security will be built into systems, such, that users are relieved of the details of assessing, testing, and developing security for that system.

3.2.4 Risk Management

DAA's will ensure that a continuing risk-management process is in effect to minimize the potential for unauthorized disclosure of sensitive information, modification or destruction of assets, or denial of service. Risk management shall be applied throughout the life cycle of the network or computer resource. DADPSSO's or NSO's will ensure the correct ADPSO approved risk-assessment method is completed as part of the accreditation process.

3.2.5 Configuration Management

Configuration Management (CM) exists because changes to complex systems and networks are inevitable. The purpose of configuration management is to ensure that these changes take place in an identifiable and controlled environment, that they do not adversely affect any properties of the system or network, or in the case of trusted systems, that they do not adversely affect the implementation of the security policy of the trusted system. The NSO and system management are responsible for assuring the following: 1) that additions or deletions to the network configuration are consistent with the security policy, 2) that audit mechanisms are modified to reflect the new environment, 3) that unauthorized network use is not supported, and 4) that password mechanisms are properly invoked.

Changes to the software configuration must assure the following: 1) that virus attacks are prevented, 2) that Trojan horse attacks are not introduced, 3) that software is within the scope and the mission of that configuration, and 4) that any obsolete versions are removed from the system.

The size and requirements of a network may change over time and periodic re-evaluation and reconfiguration of the network is needed. Configuration management provides for the optimization of all network resources and maximizing both throughput and reliability of data transmission. Configuration management includes a database

containing all the information related to the system configuration including hardware, software, and documentation elements.

3.2.5.1 Hardware CM

Provisions shall be made by the NSO to maintain a database containing all the CM information relating to the description, make, model, and version of physical equipment in the network, including:

- interface/interconnected devices
- node host systems
- PC's/terminals
- network medium (i.e., wire Ethernet, FDDI)
- ports
- configuration of each networked device;
  - modem
  - local controller
  - communication cables and connectors
- topology of networks
- geography of networks

3.2.5.2 Software CM

Provision shall be made to maintain a database containing all the information related to the description and version of software hosted on the network, including:

- network operating system
- node host computer and PC operating systems
- protocols
- application programs
- security/auditing programs

Operator/Machine Interfaces (OMI) descriptions will depict whether software programs run with the same commands both on and off the network. Also, an explanation of network commands above and beyond normal program commands is required.

3.2.5.3 Documentation CM.

Provision shall be made to maintain a database containing a listing of network CM documents depicting the following:

- accreditation
- reproducible network diagrams depicting physical layout, network nodes, and interfaces
- network specifications (data rates, performance, response time, etc.)
- network test, integration, operating plans and procedures
- network hardware manuals
  - description and specification
  - operations and maintenance
- software specification, design, test, operation and maintenance manuals (including operating systems, application software, diagnostics and benchmarks, and security software packages), licenses, protocols, firmware, and performance data
- interface specifications
- node host system specifications and provisions
- user/training manuals (including network addresses, commands, etc.)
- Memorandum Of Agreements (MOA's) with remote sites and remote network management
- network security policies and procedures
- network security accreditation documents
- network failure analysis with restoration procedures

3.2.6 Performance and Status Monitoring

Performance monitoring is a vital aspect of security administration because characteristic patterns of activity describe both normal system usage and activities characteristic of security violations. Knowing the normal patterns of activity help alert the system administrator to anomalous activity that result from covert signaling, denial of resource attacks. penetration attempts, audit tampering and unauthorized access. Performance monitoring should listen for broadcast events, for router routing anomalies, congestion of communication resources, and any other unusual activity or inactivity. Pinging (simply querying the presence of some network component) can reveal both

operational and security relevant conditions. Router reports of packets received, packets forwarded, destinations served, connectivity tables, and up time histories are vital records of security related activities.

3.2.7 Network Hardware

The hardware required to establish a network is sometimes diverse and there exist many different LAN hardware vendors all making equipment available for multiple network communications specifications (protocols) and operating environments. Fortunately, most of these vendors understand and support the requirement to provide compatibility between these equipments. In fact, current technology allows for the mix and match of network components, often making it hard to make a wrong purchase decision.

Because technology advances rapidly, it has become a cliché that the hardware is obsolete by the time of purchase. The time spent searching for the perfect system can be better spent optimizing one of many good combinations available. The best rule-of-thumb is to plan the network for optimum performance, given the present needs and budget. At the same time, plan for the network to expand, as it most certainly will. Finally, keep the configuration as simple as possible.

A Local Area Network has a minimum configuration consisting of the cable and network nodes (host computers), but, networks inevitably grow, thus increasing the total architecture. Dealing with these changes requires making choices that allow for expansion, upgrades, and modifications.

3.2.8 Contingency Planning

For mission-critical systems and networks, contingency plans shall be developed after written approval by the NRaD Information Systems Council (ISC) is obtained, and, to the maximum extent possible, tested between accreditation to ensure that they function in a reliable manner and that backup functions are in place to ensure that critical service is maintained.

DAA's are responsible for determining contingency-plan requirements for systems under their purview.

Plans shall be tested annually under realistic operational conditions to the maximum extent feasible.

If contingency plans cannot be tested realistically before accreditation, the DAA may issue an IATO pending testing within one year.

3.2.9 User Access

An AIS, network, or other computer resource will follow the "least privilege" principle (i.e., most restrictive access privilege as defined in DoD 5200.28-STD "Orange Book" [NOTAL]) so that each user is granted access to only the information to which the user is entitled because of security clearance or formal access approval, and only granted access the resources necessary to perform assigned functions. In the absence of a specific positive grant-of-access, user access privilege defaults to no access.

3.2.9.1 Administering Access Controls

Password Administration

The procedures for assigning and changing passwords for systems processing or transmitting sensitive unclassified data are as follows:

- Ensure passwords uniquely identify each system access. All passwords supplied with equipment or software must be changed before allowing users to access the system. Temporary passwords are initially assigned to new users. The user must immediately change the temporary password to one known only by the user. Password changes must be provided through interaction between the user and the system. Machine-generated, 6-character, random passwords are recommended. Positive identification of the user is required whenever the system provides a new password.
- All passwords on a system must be changed periodically (i.e., at least once per year). The user's passwords must be removed promptly upon departure of the user. Passwords must be stored in the system in non-readable and non-decodable form. Network access from a host system must be controlled so that passwords are not compromised easily by network analyzers (sniffers); passwords must be encrypted.
- Controls must be provided to limit the login-attempt rate by limiting the maximum number of login attempts before generating an exception report. An audit trail of password usage and changes should be maintained. This audit should not contain actual passwords (or password attempts) but record activity of successful login, unsuccessful login, use of password changes, and the locking of passwords that have expired.

- Five consecutive and unsuccessful login attempts should generate an immediate notification to the system manager or system operator.
- Upon successful login, each user should be provided with a report of the date and time of the user's last login and each unsuccessful login attempt to this user's ID since the last successful login.
- Ensure passwords are properly authenticated by the system whenever offered for access permission.
- Ensure passwords remain private.
- Ensure system mechanisms to operate, audit, and defend against password abuse or compromise.

3.2.10 Controlled Access Protection (CAP)

Controlled Access Protection (CAP) is a term that describes the minimum set of automated controls that should be provided to Navy AISs (i.e., discretionary access control (DAC), user identification and authentication (I&A), auditing of security relevant events, and clearing of memory and storage before reuse). CAP applies to a system and will be implemented to enforce the system-specific information protection policy; the level of assurance associated with the implementation will correspond to the local risk.

The CAP requirement applies to all Navy AISs processing General Service (GENSER) classified or sensitive unclassified information (this includes operational AIS's, those under development, or in the acquisition pipeline). This guideline applies to all platforms (e.g., tactical or mission support stand-alone microcomputer, local area network (LAN), minicomputer system, mainframe system, or any other type of networked AISs. (Note: Dedicated mode systems do not necessarily require automated access and accountability controls; however, they still require protection.)

SECNAVINST 5239.2 requires implementation of "Class C2" features/functionality on all General Service (GENSER) classified and sensitive unclassified AISs. "Class C2" is a set of criteria for evaluating the security features and level of assurance provided by a product...defined in DoD 5200.28-STD (the "Orange Book"), it does not specify or address how to implement the required security features to support system-specific information protection policies. "Class C2" applies to products, both commercially available products (e.g., operating systems, database management systems, and the like) and custom

developed software, firmware, and hardware products, and the level of trust associated with their performance.

Note

DOS-based and Macintosh© personal computers may require implementations of only a subset of CAP features; however, all AISs connected to a network asset will incorporate I&A.

3.2.11 Security Auditing

Audits are an essential aspect to system security. Auditing can consist of a range of services from minimal record keeping within a machine to a centralized, protected, write-only service on a network. The primary role of auditing is to review patterns of access. Most auditing services offer filtering of auditable events that can be adjusted to suit system and management needs. A minimum set of auditable events are provided as follows:

- Discovery of repeated attempts to bypass protection mechanisms
- Discovery of special privilege use
- Act as a deterrent against perpetrator's habitual attempts to bypass the system protection mechanisms
- Assure that even if access controls are penetrated, evidence exists to assess the damage done by the perpetrator

3.2.12 Security Tools and Techniques

Security tools can be an important component to ensuring host system and network security. Common tools that should be considered by system and network managers, DADPSSO's, and NSO's to support their mission include the following:

- Time-domain reflectometers to monitor network attachments on a LAN cable.
- Security software that searches any machine on the network for accounts that have no password.
- Security software run against each host system's operating system to ensure security vulnerabilities and deficiencies are identified and patched.
- Audits of archives to peripheral storage.
- Disseminate electronic-mail security reminders and safeguards to users and system managers.

- Ensure proper use of wipe-disk programs to completely remove user-specified files from hard disk.
- Use removable AIS media, thus allowing users to lock the media in an approved container.
- Properly set file-access permission according to user group and global security-access policy.
- The ability to identify and mark invisible files in a directory, and ability to report those files.
- Utilities that support the backup-reformat-restore requirements of periods processing.
- NSA and Navy-approved, trusted-network interfaces that support single-classification-levels-processing on a multilevel network.
- Encryption software that can be used to support transmission of sensitive unclassified data.
- Use of cryptographic equipment that can be changed with crypto.
- Key fill guns.
- Approved containers for housing operational cryptographic devices for unattended operation.

3.2.13 Interoperability

Security measures for systems that are connected to other systems through networks, or long-haul communications, will employ those technological security solutions that provide for interoperability to the maximum extent feasible.

3.2.14 Security Incident Reporting

Suspected security incidents involving NRaD networks will be coordinated between the cognizant NSO(s) and DADPSSO(s), and reported immediately to the NRaD ADPSO. The NRaD ADPSO will determine responsibility for report completion, and should a conflict arise, the ADPSO will determine who has security responsibility and authority.

3.2.15 Attachment to Common Carrier Data Transports

All communication assets that exist within an NRaD facility must be approved for operation. These communication assets must be of a suitable technology that can be audited, monitored, access controlled, configuration managed, and administered.

Attachment to common carrier services poses a different set of requirements. These additional requirements are discussed in the following paragraphs.

3.2.15.1 Computer to the Telephone Network

Attachment of end user equipment (personal computers) to the telephone networks using a modem or facsimile adapter is restricted to unclassified (i.e., no data sensitivity) attachments. All equipment attached to the telephone network and all devices attached to that equipment (including other network adapters) must be unclassified (without any data sensitivity). Attachment of machines that contain classified data, or that are attached either directly or by way of a network to any machines that contain classified data, are restricted to the use of approved STU-III equipment for attachment to data communications services. For any machines that transmit sensitive unclassified data, it is highly recommended that approved data encryption devices or software be used. See your DADPSSO for current approved products or devices.

3.2.15.2 Routers that Communicate over the Telephone Network

Routers that depend upon telephone network communications must provide cryptographic protection for data communications. If the router processes only unclassified data, then DES encryption is required. If the router processes classified information, then Navy provided CMS cryptographic equipment approved for that classification is required. The status of these communications lines should be made available to administrators for that router if possible.

3.2.15.3 ISDN Services over the Telephone Network

Integrated Services Digital Network (ISDN) services are subject to the same restrictions as router attachment since STU-III service does not support ISDN service. Approved cryptographic covers must be provided for all ISDN data and control signal paths.

3.2.15.4 Public Packet Networks

Since the use of link-encryption techniques is not applicable to public packet transport services, use of these services requires specialized packet encryption technology. Packet encryption technology requires that the data portion of the packet be

encrypted while the header portion be in the clear so that the packet(s) can be routed through the Public Packet Network. No products are yet approved for packet encryption service to cover classified data. Since packet encryption techniques are not, in themselves, capable of addressing all the necessary security issues, Public Packet Networks may never be approved for the transport of classified data, but may be approved for DES packet encryption of sensitive, unclassified data in the future. Until suitable products are approved to provide packet encryption service the use of Public Packet Networks is not supported.

3.2.15.5 Private Common Carrier Packet Networks

Attachment of NRaD communication assets to Private Common Carrier Packet Networks can be approved on a case-by-case basis. Suitable Private Common Carrier Packet Networks (PCCPN's), such as DISNET, are approved for single level service and support link encryption service on their router interconnects. The use of packet encryption techniques is required, usually in the form of BLACKER system support.

3.2.15.6 Radio Networks

Afloat communications are based on the use of radio networks to support connectivity between platforms and shore sites. These radio networks provide transport services that are protocol Government Open System Interconnect Profile (GOSIP) compliant and thus no different from land-based PCCPN's with the following exceptions:

- Radio networks can be subject to significant delays from radio relays, satellite communications, and congestion. Protocols may time out if they are not aware of the possible delays.
- Radio networks can experience error rates that terrestrial communications do not experience.
- Very often radio networks are themselves packet switching networks. Terrestrial communications are usually based on point-to-point links or circuit switching techniques, with packet switching being performed at the routers. Radio networks use either broadcast down-link techniques, or routing techniques to move from

source(s) to destination(s). The discipline that radio networks enforce among their participants can affect the delays, access to the net, and multi-destination delivery.

- The accessibility of radio networks can vary. Service can be interrupted or terminated unexpectedly.
- Radio networks often support small packet sizes so that their net cycle times are low. Small packet sizes can result in fragmentation of the user packet. Fragmentation can drastically affect user throughput.

NOTE

Other than the special circumstances noted above radio networks operate just as other PCCPNs.

3.2.16 Multi-Level Security (MLS) Environments

Multi-Level Secure networks are designed so that participants operating at their appropriate security level can share access to communication and data management resources. MLS environments depend on objects (files, packets, devices etc.) being associated with a security label. Access controls derived from DoD guidelines, local security policy and accreditation methods determine how labeled objects can be generated, stored, and communicated. MLS resource sharing environments can be developed according to two general models:

* Networks that can convey packets with a range of security markings (i.e., a label range). Hosts attached to such a network must be trusted to emit and accept packets from that network within their "accreditation range". The accreditation range can encompass one label or a label range that is contained with the label range for the environment.
* Networks that accept a security label, but whose attached hosts can contain objects that do not equal those security labels accepted by the network, must be trusted to properly relabel the information that traverses the single label network (via encryption or decryption).

Clearly, MLS networks that accept a range of security labels face different issues than MLS networks that accept only a single security label. Networks that accept a range of security labels must deal with issues of (presumably) unencrypted MLS data traversing the network and transmitting (presumably) unencrypted MLS data into attached communication links. Although the communication links may be encrypted, all recipients must be trusted to support the security policy of the data source. MLS Networks that support a single label must support trusted encryption service on each host that handles labels that do not equal the label of the network. These hosts must be trusted to be valid MLS hosts, and the encryption service on these hosts must support a viable key distribution strategy that synchronizes encryption service among participants.

The data sharing objective for developing MLS data networks is equally important to the communication sharing objective. A properly structured MLS environment will support activities to "read-down" and "write-up" information. This means that a user, who requires read access to data, will be allowed read access to that information if the security label of the user "dominates" the security label of the data. This user would, however, not be allowed to write to this data object, if the user label dominates the label of the data object. Conversely, a user would be allowed to write to a data object only if the security label of the data object dominates the security label of the user. These rules express the "simple security" property of not releasing information to lower security levels. This concept of "no read-up, no write-down" is certainly a different sense of what security meant in the past when security simply meant segregating information of different levels. In an MLS environment, trusted database servers can be configured to accept interactions with trusted users based on labeled information.

At this time, NRaD representatives are not empowered to accredit MLS networks. Special requests and documentation must be developed in concert with the Electronic Systems Security Group for MLS implementations. As trusted MLS operating systems software (i.e. trusted Solaris, trusted Xenix, trusted ATT Unix) and trusted network adapters (i.e. Verdix LAN) become more available, it is natural to assume that MLS accreditation within NRaD will become a reality.

3.2.17 Configuration Management (CM)

3.2.17.1 CM for Classified and Unclassified LANs

- All network physical and logical configurations are documented by network management or designee.
- Network management (or a designee) reviews and approves all proposed additions, changes, or deletions to network configurations prior to reconfiguring.
- The NSO reviews all proposed network configuration additions, changes, or deletions to ensure an overall stable network security posture is maintained before authorizing action to change network configuration. Each proposed network node and connectivity modification to the network must meet written network security policy for the overall network operation.
- Network management ensures each node has implemented appropriate security measures by periodically running network test programs to verify known security deficiencies are not on network node host systems; likewise, each node host system manager has responsibility to ensure that the latest system security measures are installed on their cognizant system as part of CM to the operating system software.
- The NSO must maintain full network inventory of current CM.
- Standard network protocols are implemented and managed. All protocol changes are approved by management before changes are made.
- All proposed changes made to network component equipment and software, and changes to host system equipment and software, must be verified for accuracy against actual hardware and software prior to allowing the hardware or software to be operationally used.
- CM of classified network hardware must ensure TEMPEST requirements are being met before approval is granted for additions or changes in hardware configuration. The NRaD TEMPEST Control Officer (TCO), Code 153, must be contacted for a TEMPEST visual inspection of hardware changes, before operating such hardware.

3.3 General Networks - Network Security Guidelines

3.3.1 Sensitive Unclassified Networks

3.3.1.1 Network Administration

This section briefly discusses network administration and its importance to network security. The management, implementation, support and maintenance of security mechanisms is the responsibility of network administration. Many administrative issues are security issues as well. Network administration is comprised of the following functional areas:

- Management
- Maintenance
- Monitoring
- Security
- Cost Allocation
- Services (*Name Resolution, Route Determination etc.*)
- Reachability Updating and Management Coordination among Sites
- Configuration Management
- Policy Enforcement
- Crisis Management

Enumerating the aspects of network administration illustrates how network security is integral to other aspects of network administration; for example: resource availability is both a maintenance and a security issue; traffic flow analysis is both a security and a network monitoring issue; access control, resource availability and traffic flow analysis are all security and route determination issues. Attacks on an information system can often be most successfully launched against the administration of that system. Thus, a key aspect of providing network and system security is to provide robust and secure network administration.

The methods that are evolving for administration of network systems are based on the Client Server model. The Site Manager (Administrator) operates as the client processor (shown in Fig. 3-6 as the Manager Processor) while the management Agents

are embedded within the managed assets (Bridges, Gateways, Print Servers, Server processor, User processor, etc.) at that site.

The manager processor depends on a database of configuration, status, user, security, and capabilities information. The operator consults this database of status and performance information to make decisions. This database is continually updated by a polling process that send queries to its agents that are embedded in the servers (Print Servers, Bridges, Gateways etc.) and updates the database with the responses.

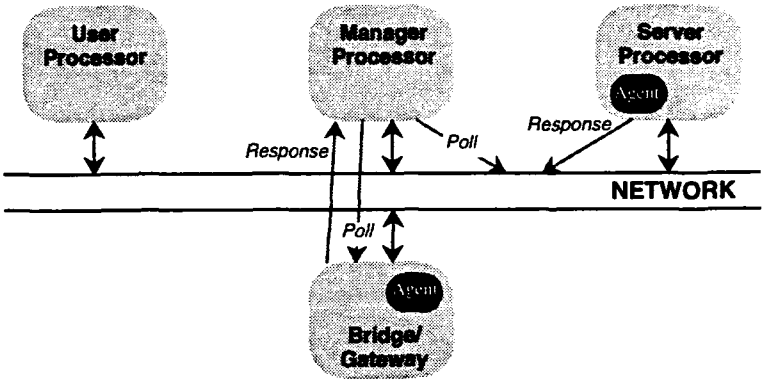


Figure 3-6
CLIENT SERVER MODEL

The Server Processor contains embedded management agent processes (See Fig. 3-6). These agent processes are produced with specific knowledge of what factors they are to monitor, and they continually update their local knowledge.

The server processors report their local knowledge to the Manager Processor whenever they are polled to do so. Formal definitions of managed objects are developed using an abstract notation that assures that the managed objects and the object manager agree on the meaning, ranges, and format of information exchanged. These formal definitions, or MIBs (Management Information Bases) are commonly available, so that Server Implementors can implement agents that the Manager Processor already knows how to communicate with them.

Protocols have been developed to support the exchange of network management information between managed objects and object managers. The dominant management protocol is the SNMP (Simple Network Management Protocol). SNMP is being enhanced so that exchanges between managed object and object managers have security properties. Security issues that network security administration deals with, are discussed in MIL-STD-2045-38000, dated 4 January 1993, "Military Standard for Network Management for DoD Communications (draft)". This structure is helpful in demonstrating how network security is integral to other aspects of network administration. Resource availability is both a maintenance and a security issue. Traffic flow analysis is both a security and a network monitoring issue. Access control, resource availability and traffic flow analysis are all

security and route determination issues. Attacks on an information system or network can most often successfully be launched against their administration process. Thus, a key aspect of network and system security is through providing robust and secure network administration.

The paradigm that is evolving for administration of network systems is the Client Server paradigm. Administration Operators and processors operate at the client processor. The client processor depends on a database of configuration, status, user, security and capabilities information. This database is continually updated by a polling process that send queries to server processors and update the database with the responses. The server processors are embedded in the managed resources throughout the network. These server processors are produced with specific knowledge of what factors they are to monitor, and they continually update their local knowledge. The server processors report their local knowledge to the client process or whenever they are polled to do so. Formal definitions of managed objects are developed using an abstract notation that assures that the managed objects and the object manager agree on the meaning, ranges and format of information exchanged. Protocols have been developed to support the exchange of network management information between managed objects and object managers. The dominant management protocol is the Simple Network Management Protocol (SNMP). SNMP is being enhanced so that exchanges between managed object and object managers have security properties.

3.3.1.2 Network Security Administration Requirements

To assist with the management of network security administration, guidelines are provided, as follows:

- A Network Manager has been identified and assigned (in writing).
- A NSO has been formally assigned and appointed (in writing). Currently assigned NSOs for major NRaD Networks are identified in Appendix C.
- NRaD NSOs must maintain liaison with all Division ADP System Security Officers (DADPSSO's) and with remote host System Managers.
- A TASO must be appointed, in writing, at all remote sites directly connected to the network.
- Backdoor connections through an on-Center NRaD network host system, or through an off-site host system interconnected to the NRaD network, must be pre-approved by the DAA and the NSO.

- Network management has identified the highest data sensitivity to be authorized on the network.
- For existing networks without a security design, security policy, or procedure, the network security design and policy must be identified, documented, and installed subsequent to network security accreditation.
- Before operation, a network must be accredited to operate, in writing, by the appropriate DAA. Each network host system must be accredited to operate before being granted network connectivity, and the accreditation must be kept current annually by host system management.
- Joint service or multiple-agency networks must be accredited jointly by their respective DAA's.
- Prior to a remote host system obtaining physical connectivity, security requirements will be agreed to in a formal Memorandum Of Agreement (MOA) that is signed by the DAA for each remote host system directly interconnected with NRaD, and the local NRaD DAA.
- Network management and NSO's must ensure standard Security Operating Procedures (SOP) are developed and written for all operational areas of the network (i.e., Network Security Policy and Procedures for operational areas; such as, network management systems, file servers, bridges, routers, hubs, and remote host systems on the network).
- Network management, host system managers, and system users must ensure that software viruses, Trojan Horses, Logic Bombs, and other deviate software are not loaded on to network controllers, network servers, network host systems, and other network components. Network management, host system managers are responsible for using appropriate virus detection and eradication software tools, and ensuring integrity of software input to network components. System users are responsible for using appropriate virus detection and eradication software tools.
- All network line analyzers and sniffer equipment will be used only by authorized personnel and controlled in areas where network components or network host systems reside. Any actual or suspected security incident must immediately be reported to the cognizant NSO, DADPSSO, or network host system management.
- All network deficiencies and vulnerabilities must be discussed as if "For Official Use Only". Use of STU-III's are highly recommended when management and network security staff converse by phone about the networks deficiencies and

weaknesses. Access control, auditing, and accounting of usage requirements must be implemented for the network and all host systems attached to the network. Network access is authorized only to users with valid user-ID and a current password. Network usage is audited and the audits regularly reviewed for unauthorized usage and identifiable network interrupts. "Exception auditing" is recommended; it only audits exceptions to normal conditions occurring on the network and the network host systems.

- The network management or NSO is responsible for regular review of network audits and responsible for taking corrective action promptly. Additionally, each host system on a network must be audited and regularly checked by system managers.
- An up-to-date "Authorized Access List" must be posted and maintained at each facility where network components and network host systems reside.
- Data packets transmitted over the network should be provided with an external and easily identifiable sensitivity markings (i.e., in the packet header, if possible).
- Provisions will be made by network management to maintain integrity and software configuration management of all software used on the network and that control network operations and network security. Backup software will be maintained and available.
- As determined by network management, a formal Contingency Plan may be required for mission-essential networks, based on availability of financial resources, personnel, and equipment resources. Plans must be approved for development by NRaD Information Systems Council (ISC). Developed plans must be annually tested.
- Uncleared maintenance personnel will not be granted unlimited network and host system access.
- If a host system on a network, or network component equipment requires repair by maintenance personnel, the device must be sanitized and physically removed from network access during such repairs until an authorized network designee verifies the repairs have been properly made. Repairs on classified network equipment and network host systems will constantly be monitored by authorized network management or their designees.
- Maintenance personnel <u>will not be granted</u> unmonitored Super-User privileges. Super-User privileges will immediately be disabled after work is completed.

- Properly cleared maintenance contractors and vendor personnel for network host systems will not be granted full network privilege or unmonitored system Super-User privilege. If full privileges are needed to successfully perform the repairs, such repairs must be constantly monitored by authorized network personnel or System Managers and properly documented for configuration management of the network and host system. Super-User privileges will immediately be disabled after work is completed.
- Vendor repair facilities that offer remote on-line maintenance and repair to sensitive unclassified network components and host systems on a sensitive unclassified network, are discouraged. If it is absolutely necessary to allow such maintenance or repair, the devices or systems to be repaired must be protected and audited at all times. Operating system software on NRaD host systems must be verified for accuracy and integrity against a backup master copy of operating system software before operation.

3.3.1.3 Communications Security

It is strongly recommended that all sensitive unclassified data transmissions be protected by use of an appropriate Navy approved encryption device, (i.e., Secure Telephone Units (STU-III), data encryption devices, or other Navy-approved cryptographic equipment, with keying material). All such encrypted connectivity and use with networks at NRaD requires prior approval from either the NRaD CMS Custodian (for cryptographic use) or NRaD STU-III Manager (for STU-III use), and approval, in writing, by the network DAA, via the NRaD ADP Security Officer.

Transmission of totally unclassified (non-sensitive) data requires no special communications safeguards.

3.3.1.4 Physical Security

All network components, cables, and host systems are physically protected by safeguards commensurate with specific written network security policy and procedures that are based upon

- Highest sensitivity of data transmissions, and data stored by the network and all of its components and host systems,
- NRaD and DoN written security policy for protecting sensitive data levels on AIS and networks,

- NRaD and DoN policy for protecting AIS resources from pilferage,
- NRaD and DoN policy for ensuring information and personnel security requirements for background checks, clearances, and need-to-know are followed based on job sensitivity.
- The highest sensitivity or classification present in the physical areas where the network is located.

All offices, labs, and rooms with unclassified network components, cables, or host systems will be locked when unattended.

All buildings that contain network components and systems will be locked at close-of-business (COB) when unattended, or physically controlled by a guard when personnel are not present and the building is left unsecured or unlocked. NRaD is always controlled by an established perimeter of guard posts and a roving guard force Center-wide. Strategically located guard posts, with armed guards, are placed where required.

Only network management or designees must be granted physical access to network controllers and management control systems.

3.3.1.5 Information and Personnel Security

All personnel with physical access to the network components and host systems will be granted access to such equipment and facilities only after required background checks are granted, based on job sensitivity.

All personnel and contractors granted network access must have need-to-know for data accessed in the performance of their job.

All AIS media produced directly from network component equipment must be properly labeled with the appropriate sensitivity label and a content label for the type of data on the media and protected as required based upon the type of data resident on the media.

All magnetic AIS media used to handle and store sensitive unclassified data on any network component equipment must be sanitized by one complete overwrite or by degaussing, prior to releasing custody of the equipment.

3.3.1.6 AIS Security

3.3.1.6.1 Environment

All network components and host systems must be operated within temperature ranges, humidity, and cleanliness specified by equipment manufacturers and within

parameters specified for facilities as established by Naval Facilities. Additionally, Appendix J of OPNAVINST 5239.1A provides mandatory environment controls for AIS operation.

3.3.1.6.2 Auditing

Audit assures that persons or processes that violate security guidelines are held accountable for their actions. Typically, only events typified as "exceptions" are audited in order to limit the amount of data collected by auditing processes. The NSO has responsibility for reviewing the audit logs and taking action against offenders that attempt repeated unsuccessful logins, attempt to operate as privileged users, or violate any security guideline on that network.

3.3.1.6.3 Access controls

Assure that Operator accounts all require password access, and that passwords meet the minimum standard for length, ambiguity, update and confidentiality. Access control of communication assets is also a major issue. Controlling access to subnets (by controlling access to Bridges, Routers etc.) controls access to the attached subnets.

3.3.2 Classified Networks

3.3.2.1 Network Administration

This section briefly discusses network administration and its importance to network security. The management, implementation, support, and maintenance of security mechanisms is the responsibility of network administration. Many administrative issues are security issues as well. Network administration is comprised of the following functional areas:

- Management
- Maintenance
- Monitoring
- Security
- Cost Allocation
- Services (Name Resolution, Route Determination etc.)
- Reachability Updating and Management Coordination among Sites
- Configuration Management
- Policy Enforcement
- Crisis Management

Enumerating the aspects of network administration illustrates how network security is integral to other aspects of network administration; for example, resource availability is both a maintenance and a security issue; traffic flow analysis is both a security and a network monitoring issue; access control, resource availability and traffic flow analysis are all security and route determination issues. Attacks on an information system can often be most successfully launched against the administration of that system. Thus, a key aspect of providing network and system security is to provide robust and secure network administration.

The methods that are evolving for administration of network systems are based on the Client Server model. The Site Manager or Administrator operates at the client processor (shown in Fig. 3-7 as the Manager Processor) while the management Agents are embedded within the managed assets (Bridges, Gateways, Print Servers, etc.) at that site.

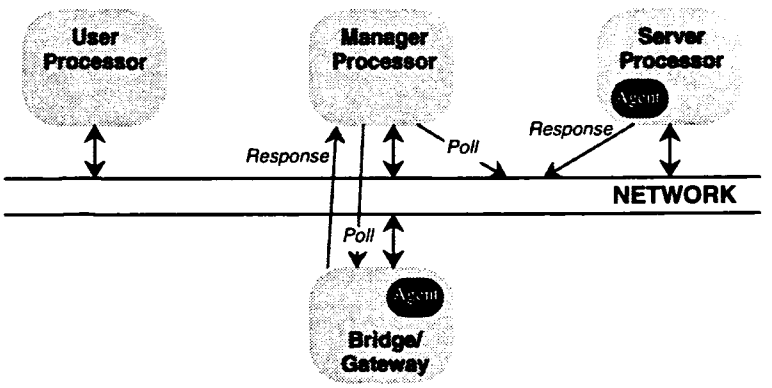


Figure 3-7
CLIENT SERVER MODEL

The manager processor depends on a database of configuration, status, user, security, and capabilities information. The operator consults this database of status and performance information to make decisions. This database is continually updated by a polling process that send queries to its agents that are embedded in the servers (Print Servers, Bridges, Gateways etc.) and updates the database with the responses.

The Server Processor contains embedded management agent processes (See Fig. 3-7). These agent processes are produced with specific knowledge of what factors they are to monitor, and they continually update their local knowledge. The server processors report their local knowledge to the Manager Processor whenever they are polled to do so. Formal definitions of managed objects are developed using an abstract notation that assures that the managed objects and the object manager agree on the meaning, ranges, and format of information exchanged. These formal definitions, or MIBs (Management Information Bases) are commonly available so that Server Implementors can implement agents that the Manager Processor already know how to communicate with.

Protocols have been developed to support the exchange of network management information between managed objects and object managers. The dominant management protocol is the Simple Network Management Protocol (SNMP). SNMP is being enhanced so that exchanges between managed object and object managers have security properties. Security issues that network security administration deals with are discussed in MIL-STD-2045-38000, dated 4 January 1993, "Military Standard for Network Management for DoD Communications (draft)". This structure is helpful in demonstrating how network security is integral to other aspects of network administration. Resource availability is both a maintenance and a security issue. Traffic flow analysis is both a security and a network monitoring issue. Access control, resource availability and traffic flow analysis are all security and route determination issues. Attacks on an information system/network can most often successfully be launched against the administration of that system/network. Thus, a key aspect of network and system security is by providing robust and secure network administration.

The paradigm that is evolving for administration of network systems is the client server paradigm. Administration operators and processors operate at the client processor. The client process depends on a database of configuration, status, user, security and capabilities information. This database is continually updated by a polling process that send queries to server processors and update the database with the responses. The server processors are embedded in the managed resources throughout the network. These server processors are produced with specific knowledge of what factors they are to monitor, and they continually update their local knowledge. The server processors report their local knowledge to the client processor whenever they are polled to do so. Formal definitions of managed objects are developed using an abstract notation that assures that the managed objects and the object manager agree on the meaning, ranges and format of information exchanged. Protocols have been developed to support the exchange of network management information between managed objects and object managers. The dominant management protocol is the SNMP (Simple Network Management Protocol). SNMP is being enhanced so that exchanges between managed object and object managers have security properties.

3.3.2.2 Network Security Administration Requirements

To assist with the management of network security administration, guidelines are provided, as follows:

- A network manager has been identified by the sponsor, and assigned, in writing, with network management responsibility
- For major NRaD networks, an NSO is assigned, in writing. NSO's must maintain liaison with all DADPSSO's and system management with resources on the network.
- A TASO must be appointed, in writing, by remote site management, and a copy of the appointment provided to the NSO.
- Network management has identified the highest authorized data classification to be used/allowed on the network.
- For existing NRaD owned or managed networks without a security design or security policy, the network security design and policy must be identified, documented, and installed for subsequent network security accreditation.
- A network must be accredited to operate by the appropriate DAA before operation. Each network host system must be accredited to operate before being granted network access and the accreditation must be kept current annually by host system management.
- Joint-service and multiple-agency networks must be accredited jointly by their respective DAA's.
- Prior to network access, security requirements will be agreed to, in writing, by the network DAA and the remote host site DAA (i.e., local senior management at remote site), by formal Memorandum Of Agreement (MOA) that is agreed to by signature of each DAA.
- Network management or NSO's must ensure Security Operating Procedures (SOP) are developed and written for all operational areas of the network (i.e., General Security Policy & Procedures for the whole network including network management systems, file servers, hubs; and security policies and procedures for remote sites on the network).
- All network controllers, network servers, network host systems, and all remote network users must ensure computer viruses are not loaded onto an AIS system or network component. Network management,

host system managers, and remote network users are responsible for using appropriate virus detection and eradication software tools.

- All network line analyzers and sniffer equipment will be used only by authorized personnel and controlled in areas where network components or network host systems reside.
- Any actual or suspected security incident must immediately be reported to the cognizant NSO, DADPSSO, or remote host system management.
- All network deficiencies and vulnerabilities must be discussed as if "For Official Use Only", or discussed at classified levels, when classified network deficiencies or vulnerabilities are involved. Use of STU-III's are highly recommended when management and network security staff converse by phone about the network.
- Access control auditing and accounting of usage requirements must be implemented for the network and all host systems attached to the network. Network access is authorized only to users with valid user-ID and a current password. Network usage is audited and the audits regularly reviewed for unauthorized usage and identifiable network interrupts. "Exception auditing" (i.e. an audit of exception events on the network and host systems) is recommended. The network management or NSO is responsible for regular review of the audits and is responsible for taking corrective action promptly. Additionally, each host system on a network must be audited and regularly checked by system managers.
- An up-to-date "Authorized Access List" must be posted and maintained at each facility where network components and network host systems reside.
- Data packets transmitted over the network should be provided with an external and easily identifiable classification marking at the highest classification level of data contained in the packet (i.e., the protocol used may have an identifiable character and location assigned in the packet header to identify the classification of data in the packet).
- Each "Finished" electronic document or file transmitted by an AIS system on the network shall contain the appropriate classification marking, the Originating Agency Determination Required (OADR) statement, and the date of the declassification for the document or file. "Working Copy" documents and files (i.e., under 90-days old), shall be transmitted with

the appropriate classification marking, a "Working Copy" marking, and the originator and date of creation.

- Provisions will be made by network management to maintain integrity and software configuration management of all software used on the network, including software that controls network operations and network security. Backup software shall be maintained and available.
- As determined by network management and based upon mission criticality and cost, a contingency plan must first be approved for development by the NRaD Information Systems Council (ISC). Upon approval, the Contingency Plan must be annually tested under actual day-to-day operational conditions.
- All uncleared personnel shall be escorted at all times in sanitized areas where the classified LAN components and host systems reside.
- Uncleared maintenance personnel will not be granted unlimited network or network system access. If a host system on a network host system or network component equipment requires repair by such maintenance personnel, the device must be sanitized and physically removed from network access during such repairs. Repairs on classified network equipment and on network host systems will constantly be monitored by authorized network management or their designees. Maintenance personnel will not be granted unmonitored Super-User privileges. Super-User privileges will immediately be disabled after work is completed.
- Properly cleared network maintenance contractors and vendor personnel for network host systems will not be granted full network privilege or unmonitored system Super-User privilege. If full privileges are needed to successfully perform the repairs, such repairs must be constantly monitored by authorized network personnel or System Managers and properly documented for configuration management of the network, host system, or both. Super-User privileges will immediately be disabled after work is completed.
- Vendor repair facilities that offer remote on-line maintenance and repair to any classified network component and host systems on a classified network node are strongly discouraged. If it is absolutely necessary to allow such maintenance or repair, the device or system to be repaired must be declassified and certified as declassified by the DADPSSO and always physically disconnected from the classified network before

connecting with the remote vendor. All operating system software on NRaD systems must be verified for accuracy and integrity against a backup master copy of operating system software before reconnecting to the classified network.

UNSECURED CONNECTIVITY TO A CLASSIFIED NETWORK OR HOST SYSTEM IS FORBIDDEN WITHOUT WRITTEN NETWORK/AIS DAA APPROVAL

- Prior to handling network components and systems as unclassified, all network components and systems that have processed, stored, handled, or displayed classified data must be certified as declassified by use of appropriate procedures in OPNAVINST 5239.1A and procedures promulgated by NRaD ADPSO.
- All classified network security accreditation documents and diagrams must, at a minimum, be marked "For Official Use Only" IAW OPNAVINST 5239.1A.

3.3.2.3 Communications Security

All classified communications connectivity between networks and network host systems require continuous protection of classified data from being physically or logically accessed, and from producing TEMPEST emanations when such classified data is transmitted through uncontrolled or uncleared areas. When any classified data is transmitted, depending on the medium used to communicate (i.e., radio wave, microwave, infrared, fiber optics, or wire), the classified data will be protected both physically and logically. Physical protection comes from restricting access to certain medium by use of an approved combination of the following; guarded buildings, secure vaults, conduit pipe for running communication wires or fiber, or certified Protected Distribution Systems (PDS's). TEMPEST-shielded enclosures and TEMPEST PDS's offer physical and TEMPEST-emanation protection when traversing from a classified area to an unclassified area. As for any electromagnetic medium that uses radio wave, microwave, infrared, or fiber-optics, protection must be provided to classified information by using encryption and decryption devices that scramble the classified data. Fiber Optics may be protected physically by use of approved fiber-optics detection systems and by the physical properties of fiber optics.

3.3.2.4 Physical Security

Physical access to classified network controllers, routers, and network management systems must be granted only to authorized network management (or designees) and must not be co-located in open multi-project labs where physical discretionary access cannot be ensured. Recommended physical safeguards are provided as follows:

- All portions of networks (i.e., fiber-optics or cables) used for classified data transmissions that pass through unsecured areas or areas where security cannot always be ensured, will be protected by an approved Protected Distribution System (PDS), that has been TEMPEST certified. Design approval must first be obtained from appropriate authority before building, locating, or using such a PDS. Additionally, all changes to PDS in use must first request for and receive written approvals before making any changes.
- When classified data must be stored on any network component or network host system, the components and the host systems must be secured in an approved strongroom, certified in writing by the NRaD Security Coordinator for the highest classification resident on the network. Strongrooms are called "Open Storage" areas for classified material; they vary in structure based on existing building structures. The Security Coordinator must be contacted for structural guidance, and for requesting certification and for yearly recertification of such areas.
- All persons (i.e., Government, contractor, visitors, custodians, etc.) must possess a valid NRaD identification to gain access into any area with AIS or networks on-Center. Escorts will be provided where needed.
- All laboratories, rooms, areas containing classified network components or network host systems must post a sign that reads:

WARNING

RESTRICTED AREA--KEEP OUT

AUTHORIZED PERSONNEL ONLY

AUTHORIZED ENTRY INTO THIS RESTRICTED AREA CONSTITUTES CONSENT TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.

INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797

- Cipher locks or card key systems may only be used by management, as discretionary access controls where network components reside or in host system facilities. Cipher locks or card key systems must not be used as primary locking devices for such areas during periods when these areas are left unattended.

3.3.2.5 Information and Personnel Security

- All personnel with physical access to the network components and host systems will be granted access to such equipment and facilities only after required background checks are granted, based on required security clearance and job sensitivity.
- All personnel/contractors granted network access must have need-to-know for data accessed in the performance of their job.
- All AIS media, produced directly from network component equipment, must be properly labeled with the appropriate sensitivity label and a content label for the type of data on the media, and protected as required, based upon the type of data resident on the media.
- All magnetic AIS media used for handling or storing sensitive unclassified data on any network component equipment must be sanitized by one complete overwrite, prior to releasing custody of the equipment.
- Network management and host system management must immediately remove network access and host system access for users who resign, retire, transfer, or are discharged or deceased. Remove network access by removing system or network user-ID's, passwords and pass-phrases.
- For any network equipment or host systems that process, handle, or transmit Top Secret data, the NRaD Top Secret Control Officer, and the NRaD ADP Security Officer (ADPSO) must be notified prior to development and operation at Top Secret.
- All personnel who are to be granted access to NRaD AIS networks or resources must first be given a background check based upon job sensitivity. Access to such equipment is granted only after a favorable background check has been obtained.
- All personnel granted physical access to network components and network host systems will be granted access only after required background checks, based on job sensitivity and classification of data to be accessed, have successfully been

performed. Network management or supervisors must ensure such background checks have been successfully performed before granting access to AIS or network resources.

- All personnel on the network must be granted access based on a certifiable need-to-know and proper clearance for the highest classification of information to be accessed on the network.
- All personnel granted physical access to areas with network components and network host systems must only be granted access based on certifiable need-to-know and proper clearance for the highest classification of information accessible in the area. Certain types and levels of classified data will require special briefings and special access on dedicated network equipment. For the handling of data such as NOFORN, NATO, SIOP-ESI, NO CONTRACT, WNINTEL, etc, the Information and Personnel Security Group can be contacted for a briefing on special requirements.
- All AIS media (AIS Media defined in OPNAVINST 5239.1A) produced directly from network component equipment and directly from connected network host systems will be properly labeled with a classification label and a content label. The Classification labels must be at the highest classification authorized on the network.
- At NRaD, all classified data that is stored or resident on network component equipment or host systems (i.e., hard disks, nonvolatile buffers) must be kept in an area Certified for Open Storage by the NRaD Security Coordinator, and approved by the Designated Approval Authority (DAA). When the classified network traverses through unprotected areas between secured buildings or spaces additional security safeguards must be employed on a case-by-case basis. Contact NRaD ADPSO for further clarification.
- All cleared contractors, who are granted access to any classified areas at NRaD, must have need-to-know for the classified data and must be contractually bound by security requirements identified in the Contract Security Classification Specification DD Form 254.
- Any network component and network host system intending to transmit, process, or handle Sensitive Compartmented Information (SCI), or other special types of classified data, must first discuss requirements with the NRaD Special Security Officer (SSO), or NRaD ADP Security Officer (ADPSO), before procuring and implementing equipment or facilities.
- All "Finished" (i.e., over 90-days old) secret AIS media and material created by a network component or host system on a network node must follow Secret Material Inventory requirements. Contact the Classified Material Control Center (CMCC) for

assistance or. the inventory and Bar Coding of such classified AIS media. All AIS media classified secret and above will be serially controlled.

3.3.2.6 AIS Security.

3.3.2.6.1 Environment

- All network components and host systems must be operated within temperature ranges specified by equipment manufacturers and within ranges specified for facilities, as established by Naval Facilities.
- Network components and network host systems must be provided appropriate fire protection equipment and appropriate sensors for detection of smoke, fire, and humidity.
- It is mandatory that all rooms, or facilities that house network component equipment, and all network host facilities be kept clean of all dust and dirt. Regular cleaning schedules must be adhered to.
- All network component equipment and host systems must be provided dependable and stable electrical power. Installation of an Uninterruptable Power Supply (UPS) may be required to ensure continuity of operation based on network management requirements.
- All network components and host systems must be operated within temperature ranges, humidity, and cleanliness specifications from equipment manufacturers and within parameters specified for facilities as established by Naval Facilities. Additionally, Appendix J of OPNAVINST 5239.1A provides mandatory environment controls for operation of systems and networks.

3.3.2.6.2 Auditing

Audit assures that persons or processes that violate security guidelines are held accountable for their actions. Typically, only events typified as "exceptions" are audited to limit the amount of data collected by auditing processes. The NSO has responsibility for reviewing the audit logs and taking action against offenders that attempt repeated unsuccessful logins, attempt to operate as privileged users, or violate any security guideline on that network.

3.3.2.6.3 Access controls

Assuring that Operator accounts all require password access, that passwords meet the minimum standard for length, ambiguity, update and confidentiality. Access control of communication assets is also a major issue. Controlling access to subnets (by controlling access to Bridges, Routers etc.) controls access to the attached subnets.

3.3.2.7 Emanations

When an unclassified network is co-located in an area with classified processing or communications, ensure that TEMPEST separation requirements for classified areas are adhered to.

Operate all unclassified network equipment and host system equipment on separate and dedicated power circuits other than those used for classified equipment.

Precautions should be taken in accordance with TEMPEST guidelines to safeguard against emanating electronic or RF signals containing classified information. These precautions are basic to accreditation of classified AIS systems.

Emanations of classified information can be minimized in accordance with the following:

- Wire cable is conducive to inductive coupling, thus promoting emanations, unless special precautions are taken, such as:
  - Specifying high-quality, jacketed, or armored cable that provides the shielding qualities to protect against emanations.
  - Enclosing the wire cable inside hardened, sealed, steel conduit that extends uninterrupted between each communicating user host system.
- The physical properties of fiber-optic cable provide for the total protection against inductive coupling.

NOTE:
Exercise care in specifying the type of cable medium to be used in the network (e.g., wire versus fiber optic).

3.4 Project Orientation

3.4.1 Special Project Considerations

NRaD has numerous interconnected labs and AIS facilities in support of Navy RDT&E. Because of these ever changing operational laboratory and computer facility environments in RDT&E it is more important then ever to manage and administer security for these facilities with the view that they will always be changing internally; however, while being changed internally, in a authorized and managed fashion to preclude security incidents, these laboratories and facilities must interact with other external NRaD command network or AIS resources IAW the established security policy set by cognizant management for those resources.

3.4.1.1 Classified System/Network (Level I) Data Classifications.

All national security information, data, and materials created and promulgated as classified in the Navy, must be accounted for and controlled on AIS or networks with Navy information security and AIS security requirements commensurate with the assigned classification being handled, transmitted, or stored. Each individual who is to be granted access to any classified data, information, or materials must have been granted a current "clearance" and possess a documented "need-to-know" in their job function. In the Navy, there exist three basic General Service (GENSER) classifications discussed in the following list. GENSER classified data should not be confused with Sensitive Compartmented Information (SCI), which has different security requirements promulgated and handled under Navy Intelligence Command (NIC)/Defense Intelligence Agency (DIA) Special Security Officer (SSO).

Level I AIS system/network GENSER classifications are as follows:

- Top Secret (*Genser only*): Unauthorized disclosure of this information could reasonably be expected to cause exceptionally grave damage to the national security.
- Secret: Unauthorized disclosure of this information could reasonably be expected to cause serious damage to the national security.
- Confidential: Unauthorized disclosure of this information could reasonably be expected to cause damage to the national security.

3.4.1.1.1 Classification Guides.

If specific handling requirements for project information are unknown or the classification of information is unknown, the possessor of such information must ensure the appropriate classification guide is checked to ensure proper handling of the information, prior to processing, storing, or transmitting such information. Contact the NRaD Information, Personnel, and Operations Security Group

3.4.1.1.2 Need-to-know.

Within each laboratory or computer facility at NRaD, it must be ensured that the Navy's information security requirements are properly administered; that is, every person to be granted access to sensitive or classified information and work areas, must have been given a required background check and received proper clearance. Possessors of classified information must determine that the individual has "need-to-know" for such information. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance. For contractors, the basic contract must identify "need-to-know" specific to the task being worked on. Laboratory and computer facility management must work in concert with custodians and originators of sensitive or classified data, to ensure that only persons with proper "need-to-know" are granted access to such information or materials.

3.4.1.1.3 Data Caveats

GENSER data may be subject to special restrictions on reproduction, dissemination, and extraction. These restrictions are termed caveats. Special warning notices or intelligence control markings should appear with this data. For specific guidance on proper handling of caveated material you should contact the NRaD Information, Personnel, and Operations Security Group. Some data caveats commonly seen on data being used at the Center are as follows:

NATO

North Atlantic Treaty Organization (NATO) data (Controlled by U.S. Registry via SPAWAR)

NOFORN

Not Releasable to Foreign Nationals

NO CONTRACT

Not Releasable to contractors or contractors consultants

WNINTEL

Warning Notice - Intelligence Sources or Methods Involved

CNWDI

Critical Nuclear Weapon Design Information

SIOP-ESI

Single Integrated Operational Plan - Extremely Sensitive Information

COMSEC

Communications Security Material

PROPIN

Caution - Proprietary Information Involved

For more information see Appendices A and B

3.4.1.1.4 Security Modes of Operation

The Navy AIS Security Program promulgates the Security Modes of Operation shown below. Based upon documented AIS Security accreditation documentation and written Security Operating Procedures (SOP's) submitted to NRaD ADP Security Officer, the correct Security Mode of Operation will be assigned by the ADPSO for systems, facilities, and networks to be operated on-Center or those networks managed by NRaD off-center. A Mode of Operation is a quick reference to identify a complex set of security criteria for operation of Navy computers or networks. The Navy's Security Modes of Operation, are as follows:

- **Dedicated Security Mode -**

  A system operates in dedicated security mode when the system and all it's connected peripherals or remote sites are exclusively used and controlled by specific users, or groups of users, having a security clearance and need-to-know for the processing of particular categories and types of classified material.

- **System High Security Mode -**

  A system operates in system-high security mode when the system and all it's connected peripherals or remote sites are protected in accordance with the requirements for the highest classification, category, and type of material contained in the system. All personnel having access to the system shall have a security clearance, but not necessarily a need-to-know for all material contained in the system. The design and operation of the system must

accordingly provide for the control of concurrently available classified material in the system on the basis of need-to-know.

- **Controlled Security Mode -**

  A system is operating in controlled security mode when at least some personnel (users) with access to the system have neither a security clearance nor a need-to-know for all classified material contained in the system. However, the separation and control of users and classified material on the basis of security clearance and security classification is not essentially under the operating system control as in multilevel security mode. (NOTE: Due to the absence of automated controls on the system for ensuring proper clearance and need-to-know for classified material, the controlled security mode is heavily reliant upon written administrative procedures and controls that must be adhered to by all personnel, monitored for adherence by management, kept up-to-date, and regular training on procedures provided to system users).

- **Multi-Level Security Mode -**

  An operation under an Operating System (Supervisor or Executive Program) that provides a capability permitting various categories and types of classified materials to be stored and processed concurrently in a system, that permits selective access to such material concurrently by uncleared users and users having differing security clearances based upon need-to-know. Separation of personnel and material on the basis of security clearance and need-to-know is accordingly accomplished by the Operating System and associated system software. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals for personnel having different security clearances and need-to-know.

- **Compartmented Security Mode -**

  For Navy purposes, the compartmented mode should be considered equivalent to multilevel security mode. Compartmented mode utilizes resource-sharing systems for concurrent processing or storage of two (or more) types of sensitive compartmented information (SCI), or processing or storage of any type of SCI with other than SCI information.

- **Limited Access Security Mode -**

  A system or network is operating in limited access security mode when the type of data being processed (or transmitted) is categorized as unclassified

and requires the implemetation of special access controls to restrict the access to the data only to individuals who by their job function have a need to access the data.

The criteria used to determine a Security Mode of Operation, includes the following:

- Highest classification or sensitivity of data processed, transmitted, stored, or handled.
- Personnel clearance and need-to-know for physical access to the system, facility, or network
- System or network access controls present
- Physical Security safeguards for a system or facility
- System, network, or facility management's written security operating procedure and policy for operation.

3.4.1.1.5 Operational Environments

Below is a cross-section of operational environments at NRaD, whose combinations and permutations are lengthy. Of the environments shown, some environments feasibly can reside within another operational environment:

- Guarded Buildings
- Unguarded Buildings
- Certified Classified Open Storage Area
- Secured TEMPEST Shielded Enclosures
- Secured TEMPEST Shielded Buildings
- Unsecured Open Office Areas
- Secured and Unsecured Labs
- Secured and Unsecured computer facilities
- Secured and Unsecured Vans
- Secured and Unsecured Bunkers

3.4.1.1.6 Contractors.

All NRaD support contractors must be contractually bound to follow Navy security requirements while working or accessing government computers and networks. NRaD managers and Contracting Officer Technical Representatives (COTR's) must ensure local security requirements are included in the basic contract and subsequent Work Orders and

Statements of Work, when appropriate. Additionally, NRaD management must properly administer contractors working on-Center to control clearances, need-to know, and contractor briefings for special access to and handling of certain data caveats.

3.4.1.1.7 Foreign Government Personnel.

All Foreign Government civilian or military personnel must receive formal written approval through the U.S. Navy approval chain prior to being granted access onto a Navy command such as NRaD to visit or work. The NRaD sponsor must work closely with the Information, Personnel, and Operations Security Group, and must provide sufficient lead-time to obtain all required approvals. No exceptions will be allowed. See Appendix B for details.

3.4.2 Network Security Management Responsibilities

3.4.2.1 Evaluation of Risk.

Under the Navy Risk Management program identified in the Navy AIS Security Program OPNAVINST 5239.1A, it is incumbent upon Navy management for networks AIS, or AIS facilities to evaluate the risk of their operation and provide sufficient cost-effective countermeasures to protect Government assets and National Security information. Evaluation of risk is also a requirement for development of systems or networks under Life Cycle Management (LCM) requirements

Identify, Assess, and Accept/Reject Risk

- Risk assessments are a formal method of identifying and documenting Navy AIS and network assets, and the threats and vulnerabilities to these assets. The Navy risk assessment is a quantitative method (i.e., it considers cost to fix, replace, or protect an asset). The risk assessment is a management tool that provides a means to assess overall risk, and provides bottom-line cost to fix or protect from known threats or vulnerabilities identified as countermeasures (i.e., countermeasures are matched to each threat or vulnerability identified). The risk assessment provides management with an identified value of return-on-investment (ROI) for implementing countermeasures.
- Upon submitting a completed risk assessment to management for Government AIS and network asset(s), management must assess the overall

risk and must make a determination that it is or is not cost effective to implement recommended countermeasures, or a subset of countermeasures. For large NRaD center-wide networks, large AIS facilities, or off-Center networks that NRaD is tasked to manage, the formal review of documented known threats and vulnerabilities, to a network or an AIS, may be made by a panel of Facility Management or a Facility Review Board. Their recommendations may be forwarded to Facility, Network, or AIS management for final decision to accept or reject identified Risks.

3.4.2.2 Configuration Management (CM)

For effective laboratory or facility management of transient AIS systems, and communication connectivity within a volatile ever-changing area, it is the responsibility of supervisors, facility managers, or project managers to ensure that configuration management (CM) controls physical spaces of laboratories and facilities. With the advent of processing, handling, storing, and transmission of classified national security information and data, CM becomes even more important to ensure Information Security requirements of proper clearance, and need-to-know. In addition, the security of important TEMPEST red and black separation controls, and shielded enclosure integrity controls, must be ensured where appropriate.

The beginning of proper CM controls, is a documented CM baseline. The baseline should contain the following:

- An appointed individual assigned CM duties, and known by all System, Facility, and Project management.
- Standardized Drawings for each facility or laboratory.
- Centralized read-only drawing database. This is an on-line, read-only database of communications drawings for the Center. This database is managed by NRaD Facility Management.
- Facility Managers and DADPSSO's are encouraged to keep local databases for historical tracking of sketches made.
- Facilities Change Request

    1. Change Review Boards must review change requests to ensure compliance with facility engineering, security, and TEMPEST requirements. Unknown answers will be actively checked with subject matter experts.

2. Short-fused change requests
   - Short-fused change requests, which are not classified, may be requested by contacting the CM point-of-contact, and the cognizant DADPSSO and NSO by Email (or hand-carried classified requests). Briefly detail the proposed connectivity, operation, physical safeguards, system safeguards, and administrative controls present.
   - After submittal of the email change request, facility management and DADPSSO's must provide follow-up documented changes originally requested by short-fused Email requests.

To assist NSO's and DADPSSO's with their CM efforts, an automated and preprogrammed CM tool (i.e., a microcomputer) is available by contacting the NRaD Electronic System Security Group. This automated tool help the user easily and quickly perform the following:

- Accreditation Forms Generation
- Sketch storage
- Signature capture
- Easily up-load communications information to a Center-Wide network database (i.e., managed by NRaD Facilities Management) for Configuration Management.

3.4.2.3 Technical Review and Steering Committee.

To facilitate new and emerging networks, AIS, and software technologies at this Center, the establishment of a Technical Review and Steering Committee is chartered to provide the following technical support:

- Evaluate new tools (hardware and software)
- Evaluate exception requests
- Supplement DADPSSO, ADPSO, and NSO selected technical expertise
- Recommend Center-wide security policy and changes
- Recommend areas for random audits based upon security concerns

- If formally approved by National Computer Security Center (NCSC), become the certifying authority for evaluating Trusted Computer Systems (TCBs), trusted networking technologies, and evaluated subsystems developed by this Center.

NOTE:
At the time of this writing, such a committee has not been chartered nor established at NRaD

3.4.2.4 Training.

Security training, at all levels of an organization, is paramount to having a successful security program. The same is true for security provided to Navy networking and AIS resources. All parts of the management/employee grid are affected, one way or another, by security training as follows:

- Management security training

  This training must encompass both Executive and middle management levels. This training must be geared to provide summary of Federal law and Navy instructional requirements in day-to-day administration of networks, AIS assets, and government data. Management training must also provide "how to" information pertinent to management controls for AIS and network security. Executive and middle managers must be trained by the ADP Security Officer (ADPSO) or the Network Security Manager (NSM) or other security groups, on security principles and requirements at NRaD. Refresher training is strongly recommended periodically.

- Security Staff training

  It is imperative that each assigned DADPSSO, NSO, and TASO is provided with up-to-date security administration and technical training in performance of their duties. This is now accomplished by DADPSSOs and NSOs attending bi-monthly DADPSSO meetings hosted by the NRaD ADPSO. The DADPSSOs, NSOs, and TASOs must be attentive to Security Advisory Bulletins and technical safeguards frequently E-mailed by the ADPSO to DADPSSOs and NSOs, and to security articles available on the NRaD Bulletin Board System (NBBS). DADPSSOs must keep appointed TASOs informed and current on new information. Additionally, immediate security staff supervisors must ensure training is budgeted for their

employees and opportunities to attend periodic security training from outside technical sources are provided.

- Employee Responsibility

  Each new and existing employee will be provided periodic AIS security and Information security training from the cognizant DADPSSO or NSO. Required annual all-hands security training is provided by the NRaD Security Officer. Each employee must keep abreast of NRaD AIS and network security instructions and notes. System users requesting AIS security accreditation will receive one-on-one security training and handouts from the Electronic Systems Security Group, and will receive a list of security safeguards. Each employee is the key to protecting Navy data.

- Other security training issues.

  It is imperative NRaD personnel (both Government and Military personnel) be provided with appropriate security training pertinent to their work area. DADPSSOs and NSOs must be responsible to provide security training for personnel concerning the following issues (which are not all inclusive):

  - Reporting incidents or suspected incidents,
  - Ensuring all personnel on-board have a proper NRaD Badge, or are escorted, and how to properly challenge unbadged or unescorted individuals
  - Ensuring personnel know security requirements and duties for providing escort in NRaD buildings.
  - Ensuring personnel know security requirements and duties for using photo equipment on-Center.
  - Obtaining prior ADPSO approval for special one time demo's of AIS or network equipment on-Center.
  - Obtaining prior ADPSO approval to operate visitor owned and supplied AIS used on-Center at conferences, shows, and special Command events.
  - Types of security training available off-Center, at other government sites, and commercial training centers.
  - New employee security training.

- Annual security training refreshers.
- Encourage group discussion about security issues unique to facilities, systems, projects, or networks.
- Removing the fear of Security.
- Security clauses in contracts.
- Evaluating AIS and network security postures.
- Practicing good Configuration Management.

- Contractors Training

  As part of the work team at NRaD, Center management, supervisors, DADPSSO's and COTR's must all ensure their support personnel working on-Center are provided with training unique to this Command, as discussed in the preceding sections.

3.4.3 Projects located in approved secure Facilities.

For project testing that requires data transmissions on a Center network extending beyond a certified secure laboratory space, a written letter of security accreditation by the Network's DAA, must be obtained from the Network management. The letter will identify the approved classification and type of data and security mode of operation to be transmitted on a network. System management must ensure all written network security policies and procedures are adhered to.

3.4.4 Security Properties

Project and facility managers must ensure basic required Navy security properties are installed and working when network usage and connectivity goes beyond a secure facility. The "*-property" (i.e., capability to ensure a classified system only writes up, and reads down, on a classified system) security principle must be adhered to for networking and classified data transmissions.

3.4.5 Multilevel Security for NRaD Projects

Multilevel security system (MLS) usage on NRaD networks must be certified as "Trusted" by the DAA, in order for the data to be transmitted. The Network DAA must ensure the Security level of "B1" (defined in DoD 5200.28-STD, called the Orange Book) is used on a system/network.

To obtain the Network DAA's written accreditation approval as a MLS, projects with MLS trusted network connectivity, as part of the project design that require

networking capability beyond a certified secure facility, must carefully document the following steps:

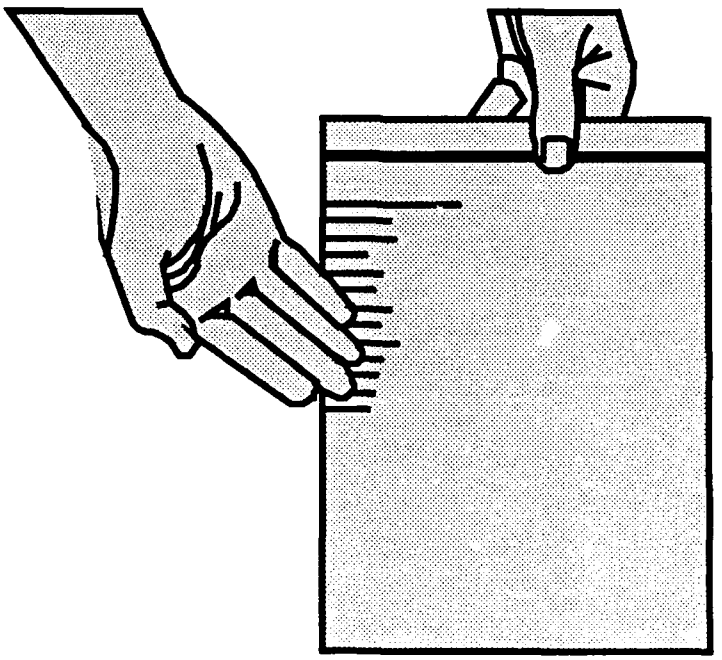
Step	MLS Operational Level	Security Environment
1	Unclassified	Secured Facility/Area
2	Classified	Secured Facility/Area
3	Classified	Unsecure Area

3.4.6 MLS Evaluated Products

A number of NSA evaluated and approved MLS products exist at this time and must be used if possible. Contact NRaD ADPSO's office, Electronic Systems Security Group, to arrange a convenient time to use this NSA reference, entitled "Information Systems Security Products and Services Catalogue", for ascertaining evaluated and certified products.

CHAPTER 4

IMPLEMENTATION



CHAPTER 4

Implementation Procedures

4.1 Network Administrator's Primer

4.1.1 Purpose

This Network Administrator's primer is designed as a quick reference for management and security personnel, to be used in the planning, design, implementation, reconfiguration, and maintenance of all NRaD network resources.

4.1.2 Intended Audience

Personnel such as; Network Security Manager (NSM), Network Security Officer (NSO), Division ADP System Security Officer (DADPSSO), and Network Management must become familiar with the contents of this primer when working with network resources at NRaD.

4.1.3 NRaD Management's Involvement with Security

Network management must not only keep senior and middle management at NRaD informed about network security design when planning network resources, they must also be informed of anticipated costs of such resources, so that sufficient budget plans may be developed to ensure the proper implementation of safeguards.

When linked together by networks, AIS resources at NRaD form a corporate entity called the "NRaD Corporate Backbone" as shown in Figure 4-1. Senior and middle management are tasked to ensure the security integrity of this integrated AIS/Network resource.

4.2 Accreditation Guidelines for NRaD Networks

4.2.1 Variations in Technology Affect Accreditation

As depicted in Figure 4-1, the NRaD Network System Diagram, networking at NRaD is comprised of many possible variations and combinations of AIS and network

technologies. When each of these technologies, with varied internal and external designs, are attached to other operational environments, a new set of operational vulnerabilities exist.

4.2.2 Definition of Network Accreditation

Network accreditation is an official written approval to operate within an acceptable security environment, as granted by a Designated Approving Authority (DAA) . DAA's are specified by the Chief of Naval Operations (CNO).

4.2.3 Accreditation Guidelines

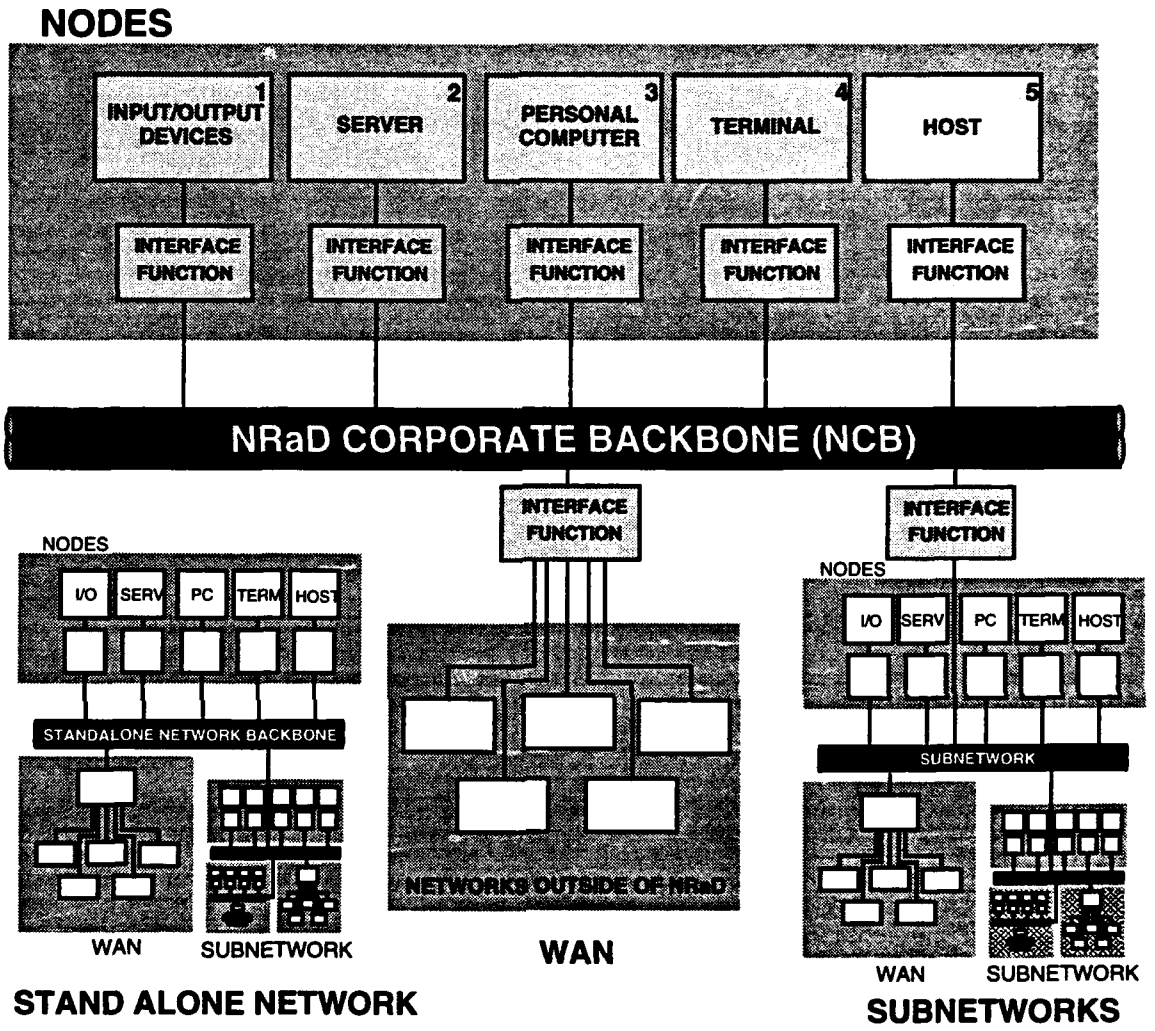
Figure 4-2, "Accreditation Guidelines for NRaD Networks", provide the six major security programs in the Navy that impact network and computer security. The DAA must evaluate an accreditation request for an acceptable level of these six security program requirements prior to granting a written approval to operate.

4.2.4 Common Security References

References used by the DAA and network management when building and operating network resources at NRaD may be found in Figure 4-3, "Background References for NRaD Network Safeguards".

4.2.4 NRaD Network Security Guidelines

Security guidelines are provided in Figures 4-4 through 4-18 and are to be used for quick reference to mandatory security safeguards and requirements found in the six DoN security programs. A more complete description of each requirement is provided in subsequent sections following the figures. Additional forms and System/Network Administrator tools may be found in Appendix D of this document.



1. **Includes video, audio, printer, & FAX scanner.**
2. **Includes storage servers, printer servers, communications servers, computer servers, etc.**
3. **Includes any and all devices with computational capability, storage and/or peripherals.**
4. **Dumb or smart terminals including peripherals (Printers).**
5. **Typically timesharing computers, mainframes, & minicomputers.**

Figure 4-1
NRaD NETWORK SYSTEM DIAGRAM

SAFEGUARDS	NODE ACCREDITATION LEVEL		
	Level I (Classified)	Level II (Sensitive UnClass)	
INFOSEC	Yes	Yes *Note 1*	NOT ALLOWED ON NCB
Physical Security	Yes	Yes	
COMPUSEC	Yes	Yes	
COMSEC	Yes	Yes *Note 2*	
Emanations Security	Yes	No	
Personnel Security	Yes	Yes	

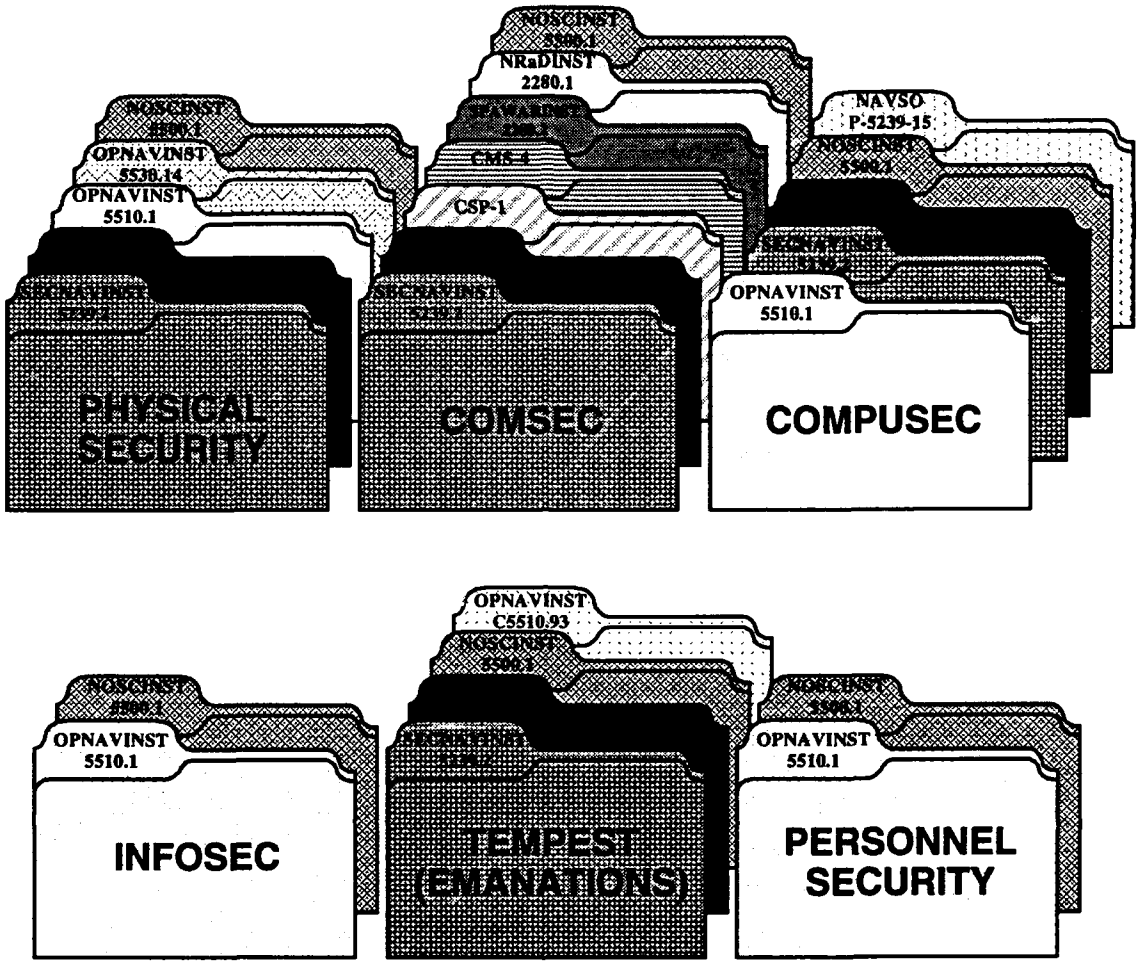
Key: Yes = Required (varies according to level)
No = Not required

NOTES:

1. Certain types of sensitive data used by the Federal Government and data protected by Public Law (i.e., Privacy Act data and/or Freedom of Information Act data) must be afforded sufficient protection levied by the law.

2. Sensitive unclassified data transmitted from the confines of this Command should be afforded protection by the use of STU-III's or other encryption devices/systems.

Figure 4.2
ACCREDITATION GUIDELINES FOR NRaD NETWORKS



SECNAVINST 5239.2	- DON Automated Information System Security Program
OPNAVINST 5239.1	- DON Automatic Data Processing Security Program
OPNAVINST 5510.1	- DON Information and Personnel Security Program
OPNAVINST 5530.14	- DON Physical Security and Loss Prevention
CSP-1	- Communications Security Policy
CMS-4	- Communications Security Material System (CMS) - Manual
SPAWARINST 2230.2	- Procedures for CMS
NRaDINST 2280.1	- Control and Operations of STU-III
NOSCINST 5500.1	- NOSC Security Manual
OPNAVINST C5510.93	- Navy Implementation of National Policy on Control of Compromising Emanations
NAVSO P-5239-15	- Controlled Access Protection (CAP) Guidebook

Figure 4.3
Background References For NRaD Network Safeguards

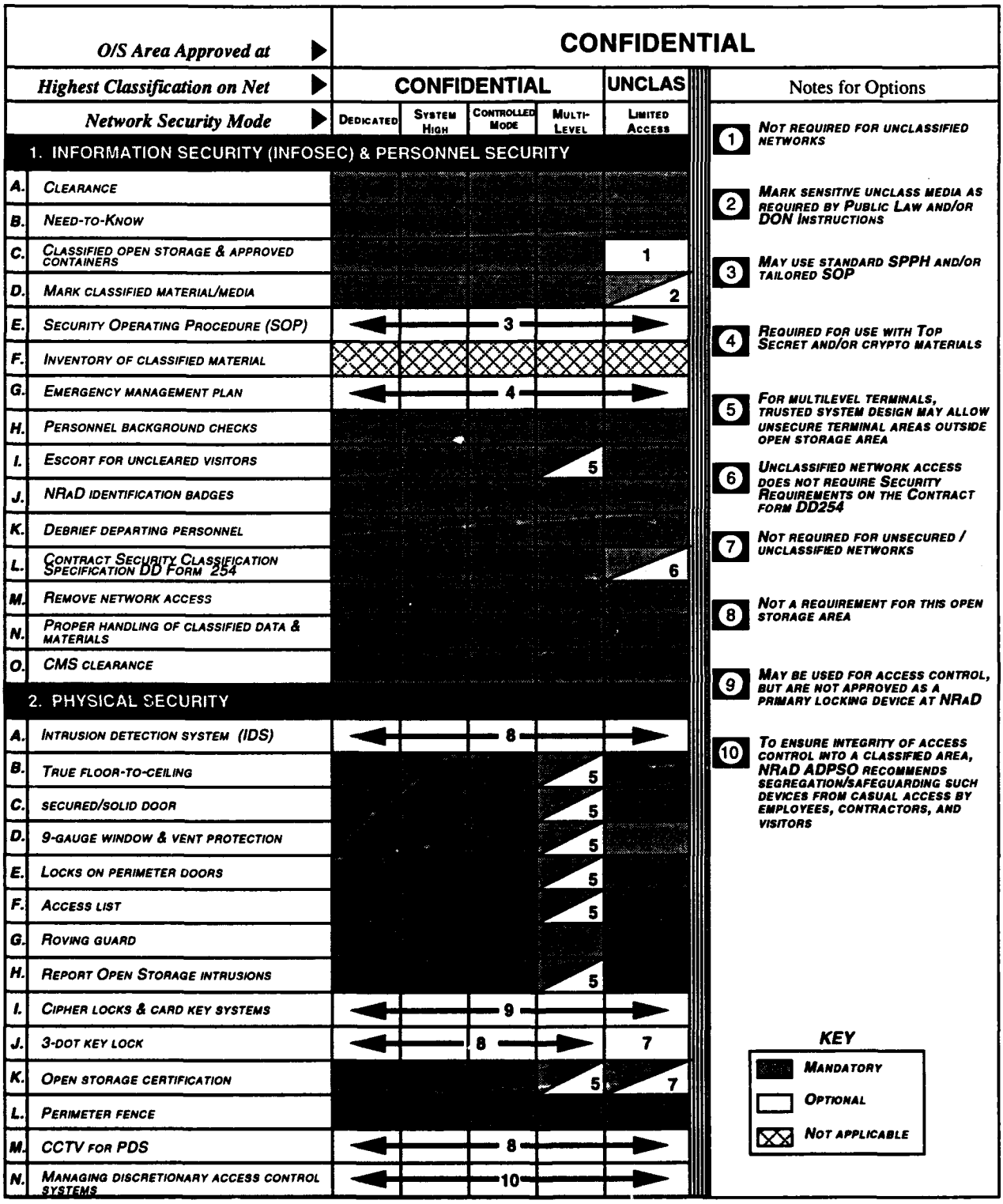


Figure 4.4
Information and Physical Security within a Confidential Open Storage (O/S) Area

NRaD NETWORK SECURITY GUIDELINE

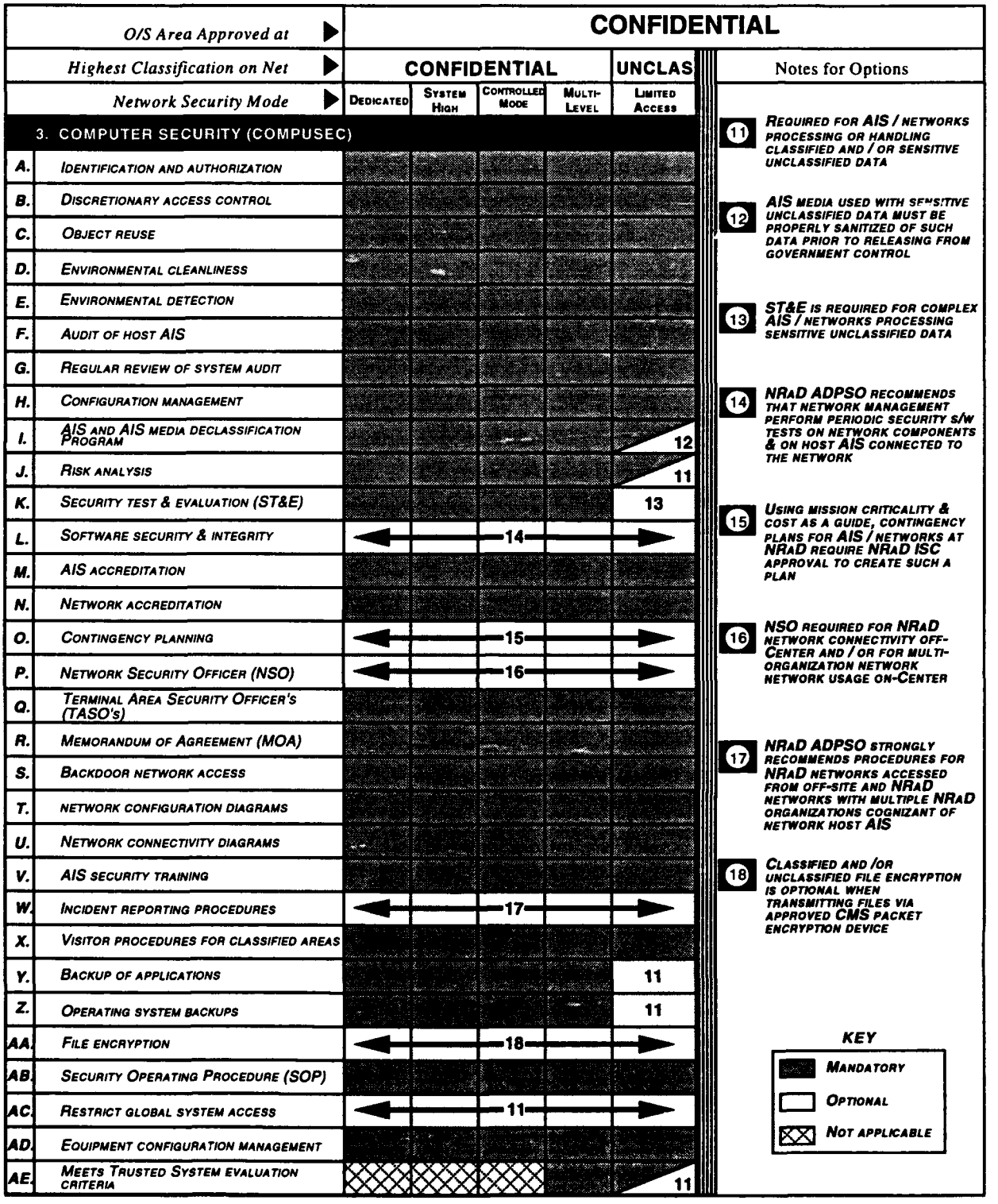


Figure 4.5
Computer Security within a Confidential Open Storage (O/S) Area

O/S Area Approved at ▶		CONFIDENTIAL					
Highest Classification on Net ▶		CONFIDENTIAL				UNCLAS	Notes for Options
Network Security Mode ▶		DEDICATED	SYSTEM HIGH	CONTROLLED MODE	MULTI-LEVEL	LIMITED ACCESS	
4. COMMUNICATIONS SECURITY							
A.	ENCRYPTION				5		① NOT REQUIRED FOR UNCLASSIFIED NETWORKS
B.	CMS EQUIPMENT PROTECTION						⑤ FOR MULTILEVEL TERMINALS, TRUSTED SYSTEM DESIGN MAY ALLOW UNSECURE TERMINAL AREAS OUTSIDE OPEN STORAGE AREA
C.	CMS KEYING MATERIAL						⑲ MAY BE REQUIRED BETWEEN USERS ON A NETWORK (OPTIONAL)
D.	TWO-PERSON INTEGRITY (TPI)						⑳ SHIELDED ENCLOSURES AND BUILDINGS REQUIRE ELECTRICAL FILTERING AND PHONE LINE FILTERING. HOWEVER, OPEN STORAGE AIS FACILITIES REQUIRE THAT A SPACE BE MAINTAINED FOR SUCH FILTERS IF REQUIRED BY HIGHER TEMPEST AUTHORITY
E.	CRYPTOGRAPHIC CLEARANCE FOR CMS MATERIAL						
F.	CMS INVENTORY						
G.	PROTECTED DISTRIBUTION SYSTEM (PDS)						
H.	DISTRIBUTION SYSTEM (DS)						
I.	STU-III'S AS CCI						
J.	STU-III'S USED WITH AIS OR FAX						
K.	COMMUNICATIONS WITH CONTRACTOR FACILITIES						
L.	PEER AUTHENTICATION	◀		19		▶	
5. EMANATIONS SECURITY							
A.	RED/BLACK SEPARATION REQUIREMENTS						
B.	TEMPEST VISUAL					1	
C.	TEMPEST SHIELDED ENCLOSURES					1	
D.	FILTERS FOR TEMPEST SHIELDED AREAS	◀		20		▶	
E.	PROTECTED DISTRIBUTION SYSTEM (PDS) CERTIFICATION					1	
F.	DISTRIBUTION SYSTEM (DS) CERTIFICATION					1	
G.	SHIELDED ENCLOSURE MAINTENANCE PROGRAM					1	
H.	RED/BLACK TRAYS FOR CABLES						
I.	SEPARATION OF POWER SOURCE						
J.	GOOD HOUSEKEEPING IN CLASSIFIED FACILITIES						
K.	GROUNDING OF TEMPEST SHIELDED ENCLOSURES						
L.	PUBLIC ADDRESS SYSTEMS						

KEY
- MANDATORY
- OPTIONAL
- NOT APPLICABLE

Figure 4.6
Communications and Emanations Security within a Confidential Open Storage (O/S) Area

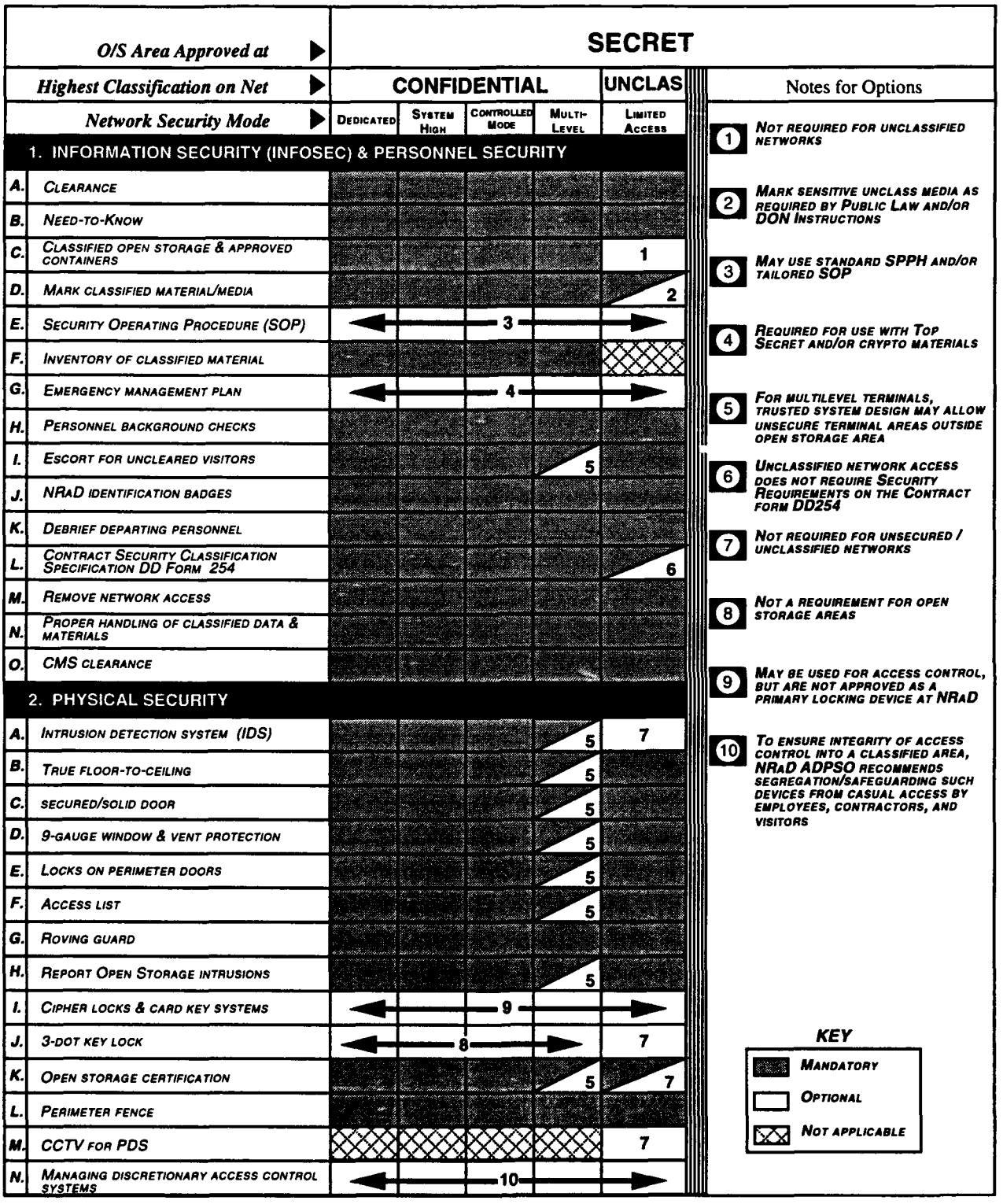


Figure 4.7
Information and Physical Security within a Secret Open Storage (O/S) Area

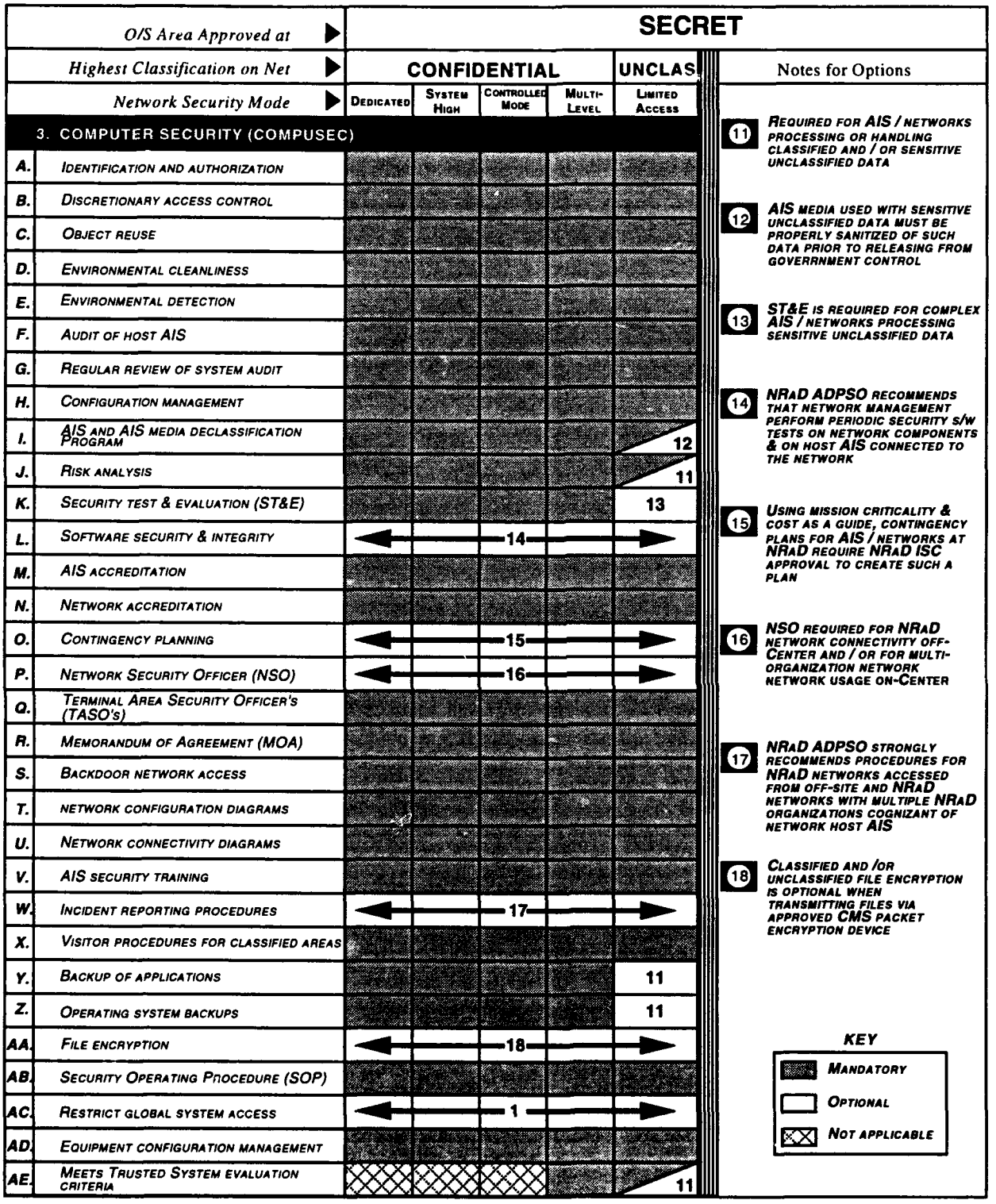
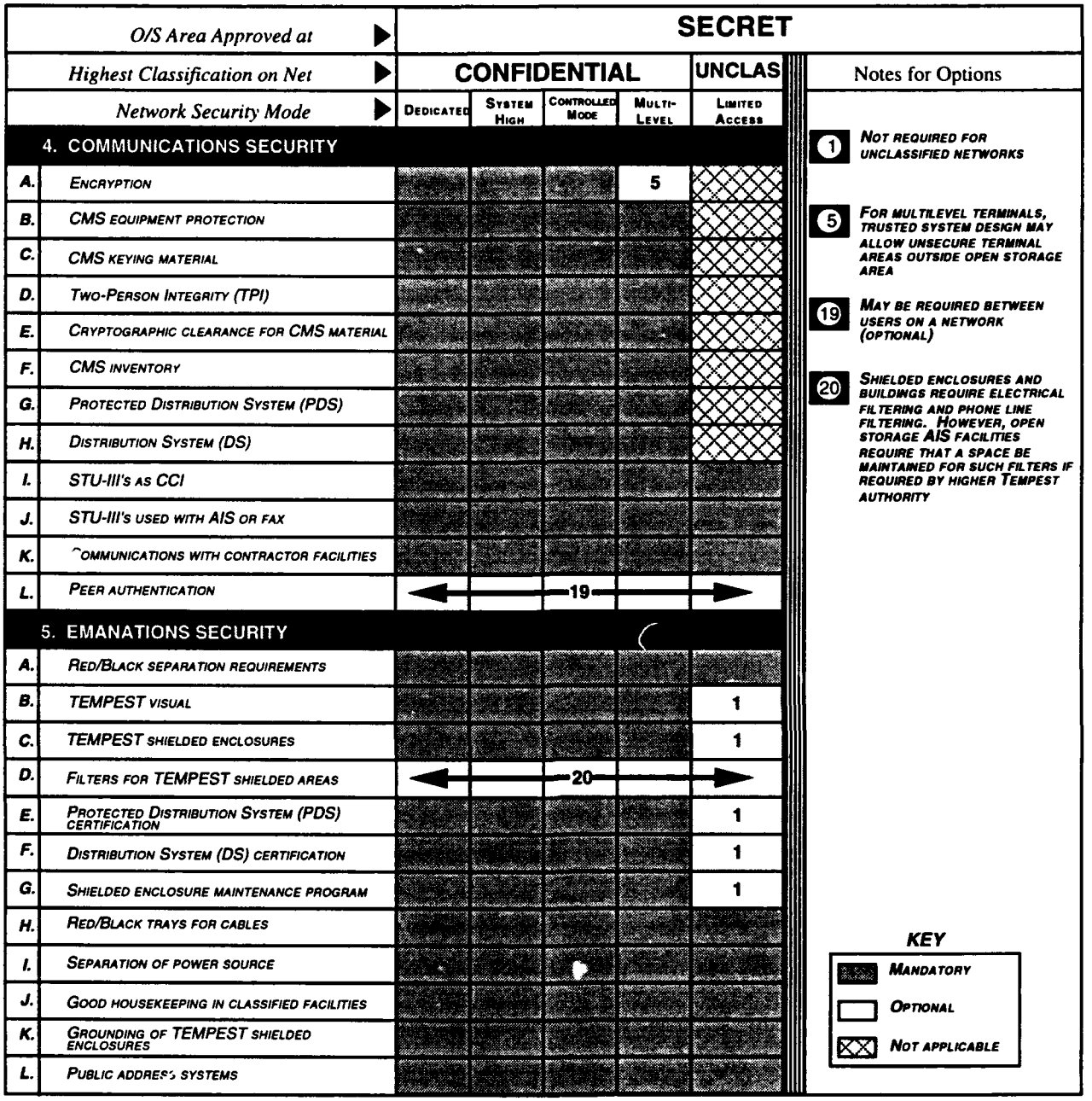


Figure 4.8
Computer Security within a Secret Open Storage (O/S) Area



O/S Area Approved at	SECRET				
Highest Classification on Net	CONFIDENTIAL				UNCLAS
Network Security Mode	DEDICATED	SYSTEM HIGH	CONTROLLED MODE	MULTI-LEVEL	LIMITED ACCESS
4. COMMUNICATIONS SECURITY					
A. ENCRYPTION				5	
B. CMS EQUIPMENT PROTECTION					
C. CMS KEYING MATERIAL					
D. TWO-PERSON INTEGRITY (TPI)					
E. CRYPTOGRAPHIC CLEARANCE FOR CMS MATERIAL					
F. CMS INVENTORY					
G. PROTECTED DISTRIBUTION SYSTEM (PDS)					
H. DISTRIBUTION SYSTEM (DS)					
I. STU-III'S AS CCI					
J. STU-III'S USED WITH AIS OR FAX					
K. COMMUNICATIONS WITH CONTRACTOR FACILITIES					
L. PEER AUTHENTICATION	◄		19		►
5. EMANATIONS SECURITY					
A. RED/BLACK SEPARATION REQUIREMENTS					
B. TEMPEST VISUAL					1
C. TEMPEST SHIELDED ENCLOSURES					1
D. FILTERS FOR TEMPEST SHIELDED AREAS	◄		20		►
E. PROTECTED DISTRIBUTION SYSTEM (PDS) CERTIFICATION					1
F. DISTRIBUTION SYSTEM (DS) CERTIFICATION					1
G. SHIELDED ENCLOSURE MAINTENANCE PROGRAM					1
H. RED/BLACK TRAYS FOR CABLES					
I. SEPARATION OF POWER SOURCE					
J. GOOD HOUSEKEEPING IN CLASSIFIED FACILITIES					
K. GROUNDING OF TEMPEST SHIELDED ENCLOSURES					
L. PUBLIC ADDRESS SYSTEMS					

Notes for Options

1. NOT REQUIRED FOR UNCLASSIFIED NETWORKS
5. FOR MULTILEVEL TERMINALS, TRUSTED SYSTEM DESIGN MAY ALLOW UNSECURE TERMINAL AREAS OUTSIDE OPEN STORAGE AREA
19. MAY BE REQUIRED BETWEEN USERS ON A NETWORK (OPTIONAL)
20. SHIELDED ENCLOSURES AND BUILDINGS REQUIRE ELECTRICAL FILTERING AND PHONE LINE FILTERING. HOWEVER, OPEN STORAGE AIS FACILITIES REQUIRE THAT A SPACE BE MAINTAINED FOR SUCH FILTERS IF REQUIRED BY HIGHER TEMPEST AUTHORITY

KEY

- MANDATORY
- OPTIONAL
- NOT APPLICABLE

Figure 4.9
Communications and Emanations Security within a Secret Open Storage (O/S) Area

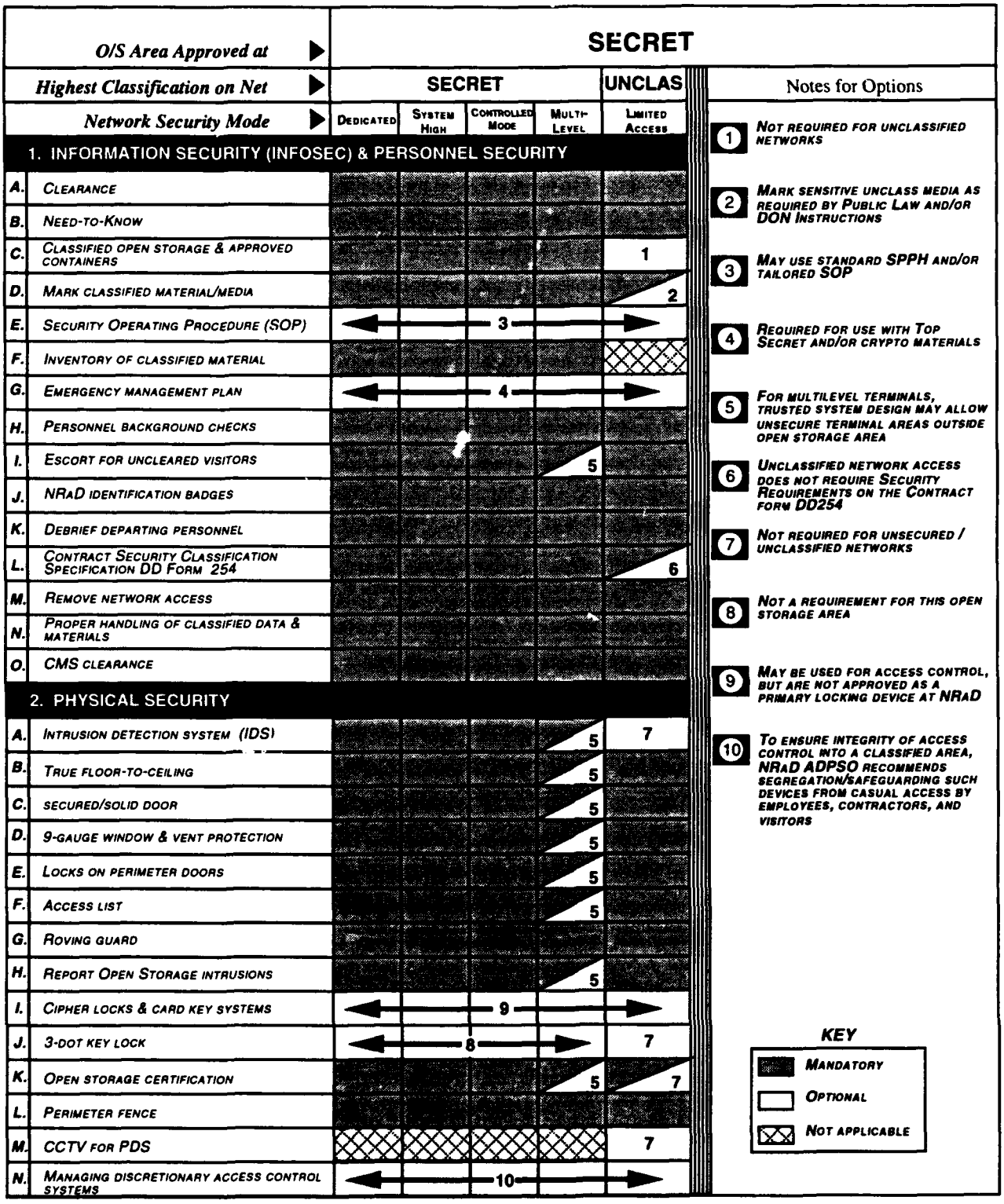


Figure 4.10
Information and Physical Security on a Secret Network within a Secret Open Storage (O/S) Area

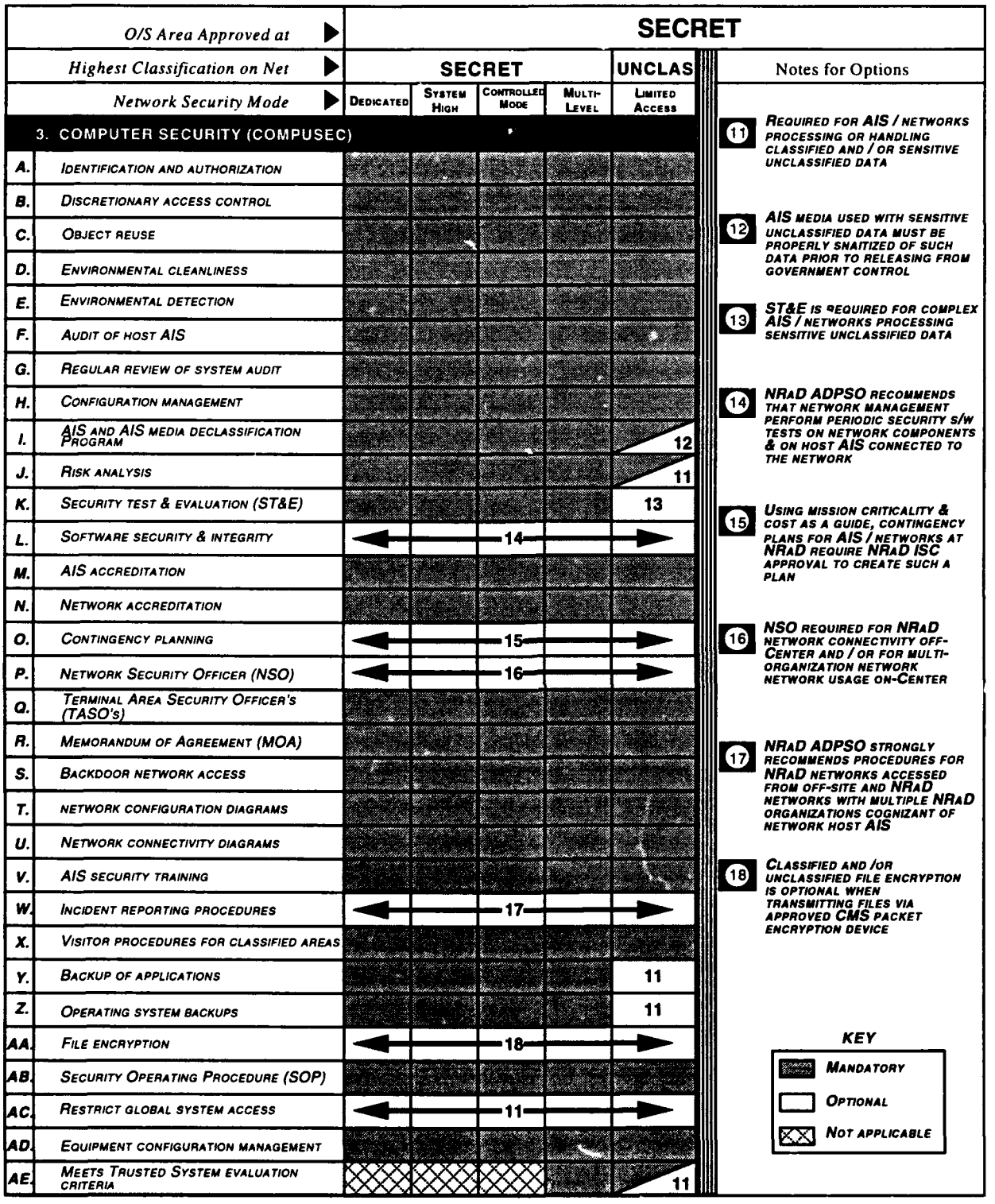


Figure 4.11
Computer Security on a Secret Network within a Secret Open Storage (O/S) Area

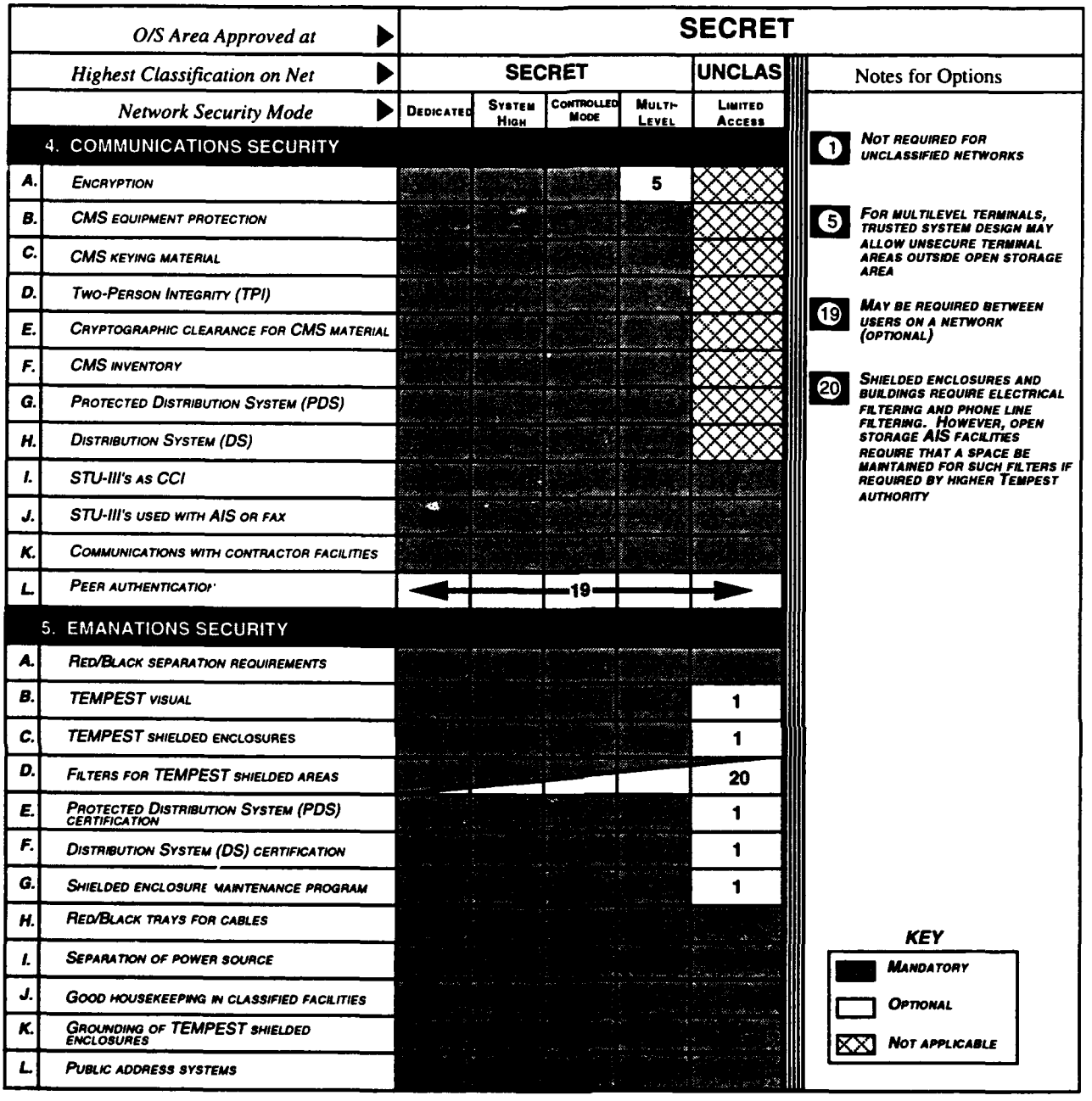


Figure 4.12
Communications and Emanations Security on a Secret Network within a Secret Open Storage (O/S) Area

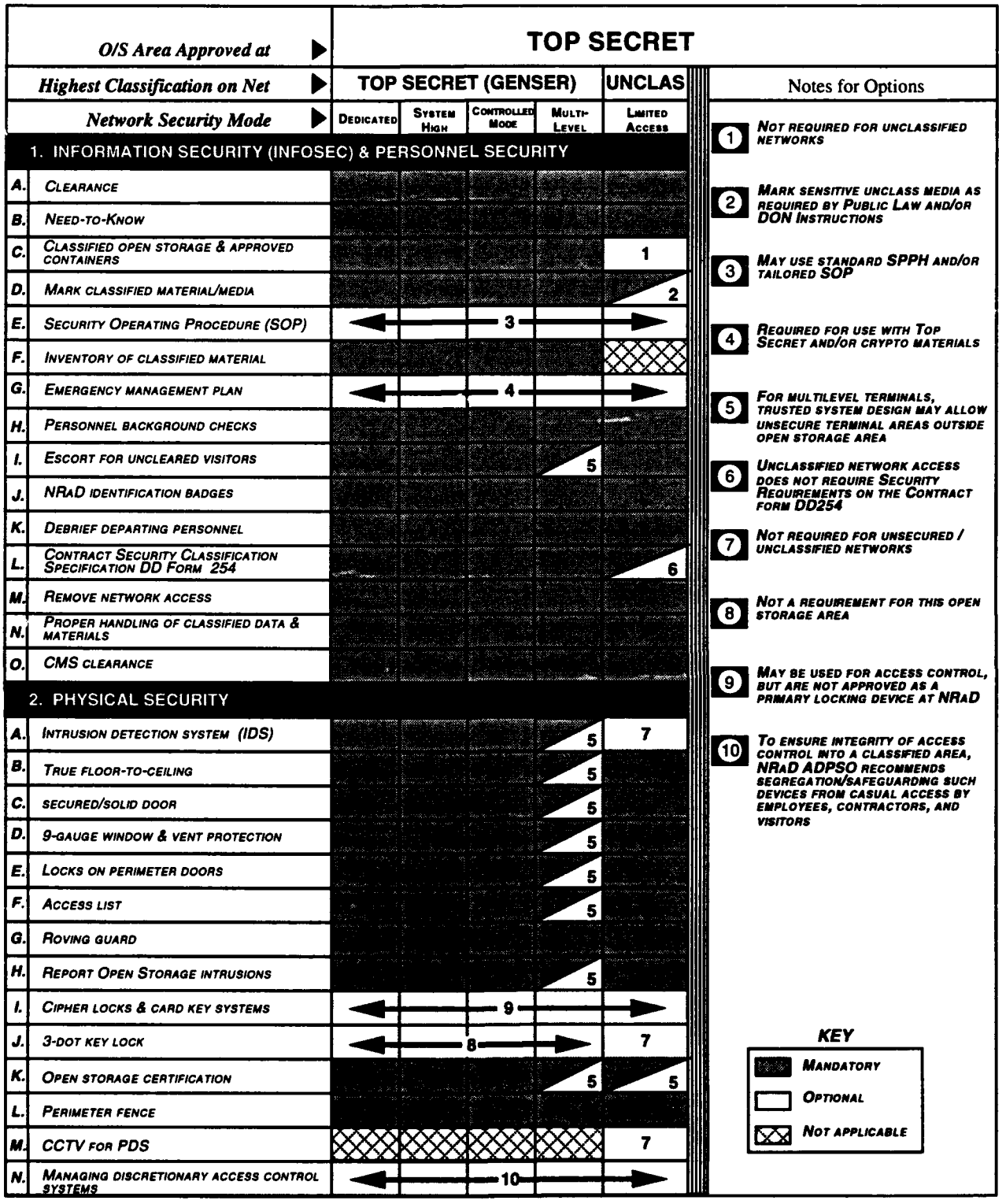


Figure 4.13
Information and Physical Security in a Top Secret Open Storage (O/S) Area

NRaD NETWORK SECURITY GUIDELINE

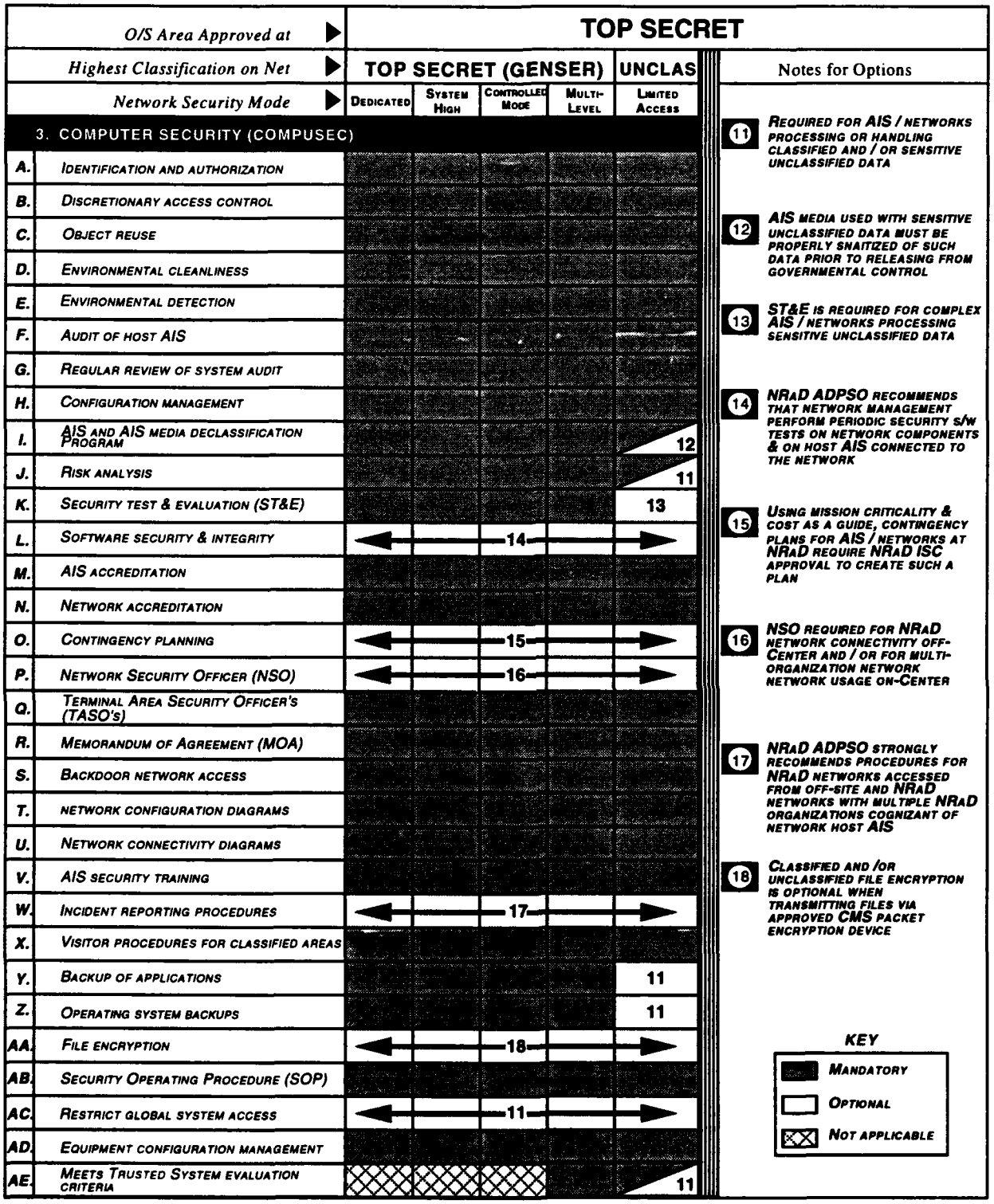


Figure 4.14
Computer Security in a Top Secret Open Storage (O/S) Area

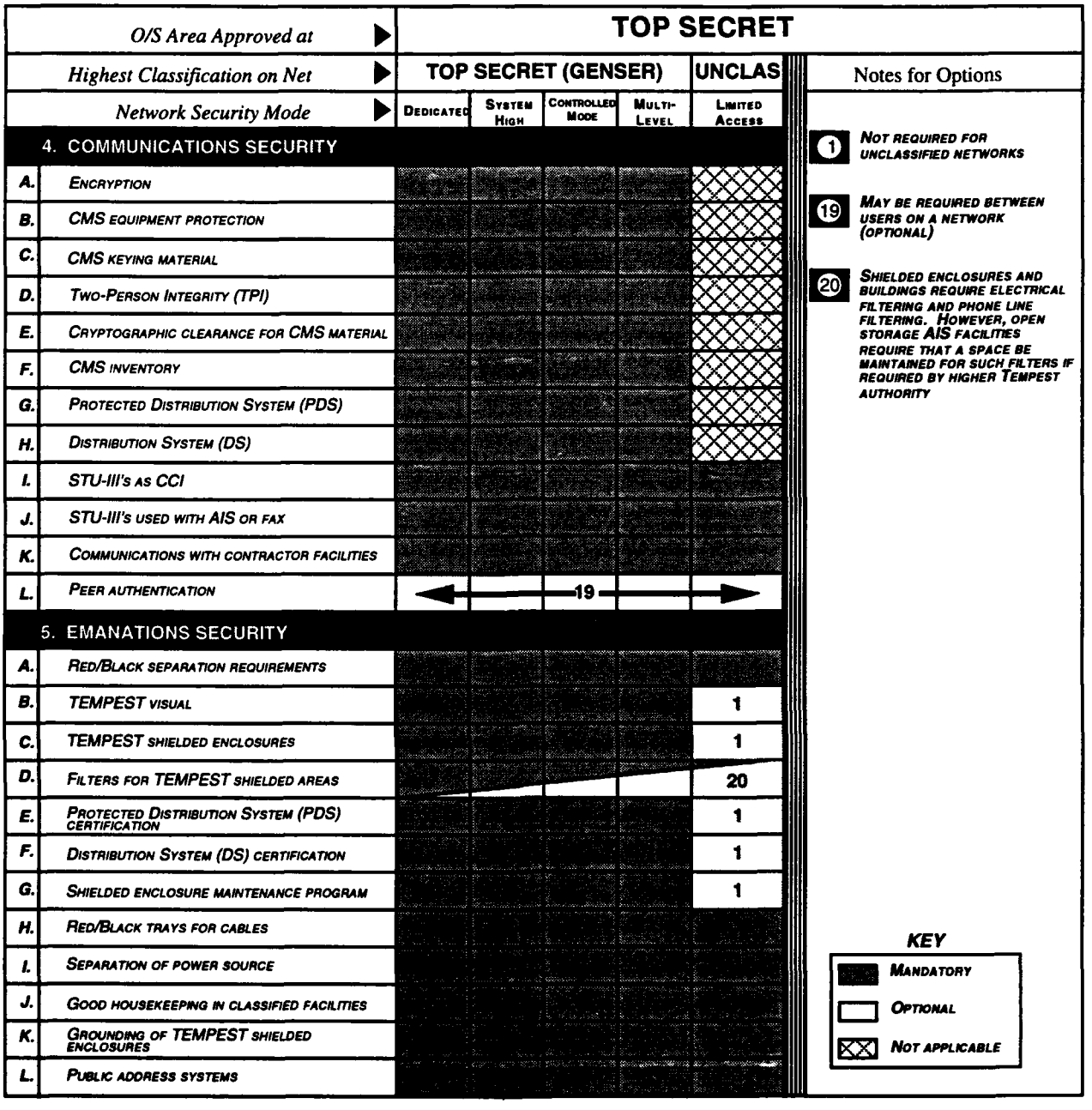


Figure 4.15
Communications and Emanations Security in a Top Secret Open Storage (O/S) Area

	Area Approved at ▶	**UNCLASSIFIED**
	Highest Classification on Net ▶	UNCLAS
	Network Security Mode ▶	LIMITED ACCESS
1.	INFORMATION SECURITY (INFOSEC) & PERSONNEL SECURITY	
B.	NEED-TO-KNOW	
C.	CLASSIFIED OPEN STORAGE & APPROVED CONTAINERS	
D.	MARK CLASSIFIED MATERIAL/MEDIA	
E.	SECURITY OPERATING PROCEDURE (SOP)	7
H.	PERSONNEL BACKGROUND CHECKS	
J.	NRaD IDENTIFICATION BADGES	
K.	DEBRIEF DEPARTING PERSONNEL	
M.	REMOVE NETWORK ACCESS	
N.	PROPER HANDLING OF CLASSIFIED DATA & MATERIALS	
2.	PHYSICAL SECURITY	
E.	LOCKS ON PERIMETER DOORS	
F.	ACCESS LIST	21
G.	ROVING GUARD	
I.	CIPHER LOCKS & CARD KEY SYSTEMS	9
J.	3-DOT KEY LOCK	7
L.	PERIMETER FENCE	
N.	MANAGING DISCRETIONARY ACCESS CONTROL SYSTEMS	

Notes for Options

(7) NOT REQUIRED FOR UNSECURED / UNCLASSIFIED NETWORKS

(9) MAY BE USED FOR ACCESS CONTROL, BUT ARE NOT APPROVED AS A PRIMARY LOCKING DEVICE AT NRaD

(21) PHYSICAL ACCESS LIST REQUIRED FOR ACCESSING SENSITIVE UNCLASSIFIED AIS/NETWORK ONLY

KEY

MANDATORY

OPTIONAL

NOT APPLICABLE

Figure 4.16
Information and Physical Security within an Unsecured Area

NRaD NETWORK SECURITY GUIDELINE

	Area Approved at ▶	**UNCLASSIFIED**
	Highest Classification on Net ▶	UNCLAS
	Network Security Mode ▶	LIMITED ACCESS
3.	COMPUTER SECURITY (COMPUSEC)	
A.	IDENTIFICATION AND AUTHORIZATION	
B.	DISCRETIONARY ACCESS CONTROL	11
C.	OBJECT REUSE	11
D.	ENVIRONMENTAL CLEANLINESS	11
E.	ENVIRONMENTAL DETECTION	11
F.	AUDIT OF HOST AIS	11
G.	REGULAR REVIEW OF SYSTEM AUDIT	11
H.	CONFIGURATION MANAGEMENT	11
I.	AIS AND AIS MEDIA DECLASSIFICATION PROGRAM	12
J.	RISK ANALYSIS	11
K.	SECURITY TEST & EVALUATION (ST&E)	13
L.	SOFTWARE SECURITY & INTEGRITY	14
M.	AIS ACCREDITATION	
N.	NETWORK ACCREDITATION	
O.	CONTINGENCY PLANNING	15
P.	NETWORK SECURITY OFFICER (NSO)	16
Q.	TERMINAL AREA SECURITY OFFICER'S (TASO's)	
R.	MEMORANDUM OF AGREEMENT (MOA)	
S.	BACKDOOR NETWORK ACCESS	
T.	NETWORK CONFIGURATION DIAGRAMS	
U.	NETWORK CONNECTIVITY DIAGRAMS	
V.	AIS SECURITY TRAINING	
W.	INCIDENT REPORTING PROCEDURES	17
Y.	BACKUP OF APPLICATIONS	11
X.	OPERATING SYSTEM BACKUPS	11
AA.	FILE ENCRYPTION	18
AB.	SECURITY OPERATING PROCEDURE (SOP)	
AC.	RESTRICT GLOBAL SYSTEM ACCESS	11
AD.	EQUIPMENT CONFIGURATION MANAGEMENT	11

Notes for Options

(11) REQUIRED FOR AIS / NETWORKS PROCESSING OR HANDLING CLASSIFIED AND / OR SENSITIVE UNCLASSIFIED DATA

(12) AIS MEDIA USED WITH SENSITIVE UNCLASSIFIED DATA MUST BE PROPERLY SANITIZED OF SUCH DATA PRIOR TO RELEASING FROM GOVERNMENT CONTROL

(13) ST&E IS REQUIRED FOR COMPLEX AIS / NETWORKS PROCESSING SENSITIVE UNCLASSIFIED DATA

(14) NRaD ADPSO RECOMMENDS THAT NETWORK MANAGEMENT PERFORM PERIODIC SECURITY S/W TESTS ON NETWORK COMPONENTS & ON HOST AIS CONNECTED TO THE NETWORK

(15) USING MISSION CRITICALITY & COST AS A GUIDE, CONTINGENCY PLANS FOR AIS / NETWORKS AT NRaD REQUIRE NRaD ISC APPROVAL TO CREATE SUCH A PLAN

(16) NSO REQUIRED FOR NRaD NETWORK CONNECTIVITY OFF-CENTER AND / OR FOR MULTI-ORGANIZATION NETWORK NETWORK USAGE ON-CENTER

(17) NRaD ADPSO STRONGLY RECOMMENDS PROCEDURES FOR NRaD NETWORKS ACCESSED FROM OFF-SITE AND NRaD NETWORKS WITH MULTIPLE NRaD ORGANIZATIONS COGNIZANT OF NETWORK HOST AIS

(18) CLASSIFIED AND /OR UNCLASSIFIED FILE ENCRYPTION IS OPTIONAL WHEN TRANSMITTING FILES VIA APPROVED CMS PACKET ENCRYPTION DEVICE

KEY

- MANDATORY
- OPTIONAL
- NOT APPLICABLE

Figure 4.17
Computer Security within an Unsecured Area

Area Approved at ▶		**UNCLASSIFIED**
Highest Classification on Net ▶	**UNCLAS**	Notes for Options
Network Security Mode ▶	LIMITED ACCESS	
4. COMMUNICATIONS SECURITY		
A.	ENCRYPTION	
B.	CMS EQUIPMENT PROTECTION	
C.	CMS KEYING MATERIAL	
F.	CMS INVENTORY	
I.	STU-III'S AS CCI	
J.	STU-III'S USED WITH AIS OR FAX	22
K.	COMMUNICATIONS WITH CONTRACTOR FACILITIES	
L.	PEER AUTHENTICATION	22
5. EMANATIONS SECURITY		
A.	RED/BLACK SEPARATION REQUIREMENTS	
B.	TEMPEST VISUAL	
C.	TEMPEST SHIELDED ENCLOSURES	
D.	FILTERS FOR TEMPEST SHIELDED AREAS	
E.	PROTECTED DISTRIBUTION SYSTEM (PDS) CERTIFICATION	
F.	DISTRIBUTION SYSTEM (DS) CERTIFICATION	
G.	SHIELDED ENCLOSURE MAINTENANCE PROGRAM	
H.	RED/BLACK TRAYS FOR CABLES	
I.	SEPARATION OF POWER SOURCE	
J.	GOOD HOUSEKEEPING IN CLASSIFIED FACILITIES	
K.	GROUNDING OF TEMPEST SHIELDED ENCLOSURES	
L.	PUBLIC ADDRESS SYSTEMS	

(22) MAY BE REQUIRED BETWEEN USERS ON A NETWORK (OPTIONAL)

KEY

- MANDATORY
- OPTIONAL
- NOT APPLICABLE

Figure 4.18
Communications and Emanations Security within an Unsecured Area

4.2.1 Information Security (INFOSEC) and Personnel Security

A. Clearance

A personnel security clearance is an administrative determination that an individual is eligible for access to classified (information at a specified level of classification). A clearance is granted to personnel (employees, contractors, students, and visitors) based upon a successful background check pertinent to the intended job position sensitivity or to the classification of information to be accessed by the personnel at this Center. For NRaD employees, this requirement is documented in NOSC-SD 5500.1 and Personnel Position Description (PPD) NRaD 5521/10.

B. Need-To-Know

To be granted access to sensitive unclassified or classified data, personnel must have a certified need-to-know for such data. A cognizant custodian, supervisor, or manager for such data, may grant approval for personnel to access such data in performance of their duties.

C. Classified Open Storage and Approved Containers

Classified data and materials may be stored in a certified strongroom, called a Classified Open Storage Area, which has met specific required physical safeguards. Classified Open Storage certification must be granted in writing by the Security Operations Coordinator.

Approved Containers are generally used to store all classified data, information, and materials. Approval of Containers is based upon the highest classification to be stored in the container, and is also based upon the environment when proper clearance and need-to-know are to be ensured for stored classified materials. Containers are accounted for by the Physical Security Group and contents are inventoried periodically by the Information, Personnel, and Operations Security Group.

D. Mark Classified Material/Media

Magnetic media containing classified data, including working copies, must be labeled on the outside, and internally, to show the highest security classification contained on the media. A data description label will also be used. Media must show date created.

Printouts, plots, and other hard copy must have the appropriate security classification marked at the top and bottom center of each page. Declassification instructions will be marked at the bottom of the first page. Hard copies must show the date created.

Classified working papers will be marked at the top and bottom center with appropriate security classification, working papers indicator and date created.

Magnetic media containing Sensitive Unclassified data must have a label affixed to the outside that indicates the appropriate sensitivity level of the data (e.g., For Official Use Only, Limited Distribution).

Hard-copy containing Sensitive Unclassified data will have the appropriate sensitivity level marked at the bottom on the outside of the front cover (if any), on the first page, on the back page, and on the outside of the cover (if any).

Magnetic media containing Privacy Act data must have "Personal Data - Privacy Act of 1974" clearly labeled on the outside of the media.

Printed output containing personal data must have the Privacy Act marking, as shown above, on the top of each page.

All sensitive Unclassified material will be locked away in a secure container (e.g., locked desk, locked cabinet) when the work space is unattended.

E. Security Operating Procedure (SOP)

For AIS with classified network access, an AIS custodian or user must provide the ADPSO with a brief written Security Operating Procedure (SOP) for the AIS accreditation, to describe the actual or unique AIS operational security environment necessary to protect the classified AIS and network, when the actual security operational environment is not covered in the Standard Security Policy and Plans Handbook (SPPH). The SOP with SPPH, must be kept at or near an AIS area, or within a facility and available for reference to by all AIS users.

NRaD managed networks with multiple organizational sites, must have a written Network Security Policy and Plans Handbook (NETSPPH) to identify network security operational and management controls, and the NETSPPH is required when requesting network accreditation from the appropriate Designated Approval Authority (DAA). The ADPSO may be contacted to obtain a NETSPPH outline or example.

F. Inventory of Classified Material

All classified Secret data, media and material that is consider finished media over 90-days old, must be entered into the secret inventory Classified Material Control Center (CMCC). Working Copy data, media, and material that is less than 90-days old, must be controlled by the custodian of the material, IAW Appendix C of OPNAVINST 5239.1A and OPNAVINST 5510.1H.

For all classified Top Secret data, media, and materials the Top Secret Control Officer must be contacted before processing, handling, transmitting, or storing this classification. A Top Secret material inventory must be maintained with the Top Secret Control Officer.

G. Emergency Management Plan

NRaD handles classified information and is required to have a Center-wide Emergency Management Plan by the NRaD Security Officer. Such a plan is being developed by the Safety Office for the protection of personnel, NRaD resources, and classified material in case of natural disaster, civil disturbance or enemy action. For classified NRaD networks, with remote sites located outside the United States and its Territories, and all deployable commands, it must be ensured that the destruction of classified information and the termination of classified network transmissions are addressed in the remote site's required Emergency Destruction Plan. An Emergency Destruction Plan may be part of the remote sites Emergency Plan

NRaD uses Communications Security (COMSEC) material, and additional emergency destruction policy and guidance must be followed, as found in CSP-1 (NOTAL).

H. Personnel Background Checks

All employees working at NRaD must be given a successful background check based upon the intended job sensitivity or classification to be accessed while employed at this Center. It is the responsibility of the supervisor to notify the Information, Personnel, and Operations Security Group whenever an employee's job duties, position sensitivity, or security clearance change. This notification is effected by submission of an updated Personnel Position Description (PPD), NRaD 5521/10.

I. Escort for Uncleared Visitors

All visitors without proper clearance or a need-to-know for NRaD classified Open Storage Areas, or other areas considered as Restricted Areas where classified material is processed, handled, stored, or transmitted from, must be escorted in these locations at all times by designated personnel. Prior to authorizing these visitor access to such areas, the entire area must be sanitized of all classified materials.

J. NRaD Identification Badges

All NRaD and tenant command personnel, PWC, contractors, and visitors must possess a current NRaD issued identification badge (permanent photo or temporary badge) to be within NRaD's perimeter and buildings, except when under the direct escort of an employee, or accessing unrestricted spaces, such as the Civilian Personnel Office, the ID/Access Administrative Services Group Control/Badge and Decal Group, and publicly accessed parking lots and roads. All personnel within NRaD that possess a current "ESCORT REQUIRED" badge, must be escorted at all times by authorized personnel.

K. Debrief Departing Personnel

Departing personnel with clearances and access to classified information, AIS, and networks, must be debriefed by their Division ADP System Security Officer (DADPSSO), and the Information, Personnel, and Operations Security Group prior to their departure from NRaD's employment. Contractors must be debriefed, as appropriate, by the NRaD Contracting Officer's Technical Representative (COTR) and by Defense Investigative Service (DIS). Personnel with clearance above Collateral data (also known as GENSER data) must be debriefed by the cognizant NRaD authority for that information.

L. Contract Security Classification Specification, DD Form 254

All NRaD contracts that will require contractors to create, handle, store, control, destroy, or distribute classified data and materials, must have all the security responsibilities fully identified on the contract security classification Specification, Form DD254, prior to being granted access to such classified data and material. All required clearances and briefings for access to certain data caveats, likewise, must be identified on Form DD254, prior to being given access to such data and materials. NRaD (O/P) 5500/3 (sample attached to Appendix A) is the Center's local implementation.

M. Remove Network Access

As part of the departing personnel checkout process for departing personnel, the cognizant Division ADP System Security Officer (DADPSSO) is notified at checkout and the DADPSSO must take steps to ensure access to all NRaD and remote AIS and networks are properly removed.

N. Proper Handling of Classified Data & Materials

The cognizant DADPSSO must ensure all personnel with access to NRaD AIS and networks have been briefed on proper handling of classified information and materials. Personnel must receive yearly training on Information Security.

O. CMS Clearance

All personnel and contractors that will be accessing areas containing material, controlled by the Communications Security Material System (CMS), must first be properly cleared for CMS access, and must follow CMS security procedures when accessing, controlling, or disposing of such material. Contractors must contractually be approved to access CMS material prior to being granted such access. Contact NRaD CMS Custodian to obtain pertinent Communication Security Policy (CSP-1) guidance for proper handling of CMS material.

4.2.2 Physical Security

A. Intrusion Detection System (IDS)

An appropriate IDS zone alarm must be installed for classified Open Storage areas that will contain classified Secret (and above) material and information. As part of an IDS zone alarm, a motion detector may be installed. Optionally, infrared detectors may be installed as part of the system.

B. True Floor-to-True Ceiling

Classified Open Storage areas require all walls to be double-wall construction, or steel, and must be extended true-floor to true-ceiling. An extension of 9-gauge, expanded steel may be used to extend a wall to true-floor and true-ceiling. Fasteners for the expanded steel must be tamper-proof; or be tack-welded to preclude surreptitious

removal. All portions of the drop ceiling or raised floor must remain in place to prevent line-of-sight into the protected area. Construction technique must be within guidelines specified by the Physical Security Group.

C. Secured/Solid Door

Doors for classified Open Storage areas are required to be solid-core wood, with hinges on the inside of the space or be protected by set-screws, hinge pins or other approved means to prevent removal. A Group 1R three tumbler combination lock must be installed and utilized on all doors used for ingress and egress. Doors to be used for emergency exit, may only be secured with appropriate hardware on the inside; if hardware is not on the outside of the door, and the door is constructed properly, a combination lock is not required. Doors that are not to be utilized at all, must be bolted to the frame in such a way as to configure part of the wall.

D. 9-Gauge, Steel Mesh Window and Vent Protection

All windows in classified Open Storage Areas must be opaque on both sides, and protected with 9-gauge, expanded steel screen. Fasteners or mounting bolts must extend through the supporting wall and be tack-welded to prevent removal. All vents opening into the space, or extending through the space, of an area of 96-square inches or more, must be protected. Steel mesh (9-gauge) or 1/2 inch steel bars must be installed to prevent access into the area. Line-of-sight must be prevented into the protected area; this can usually be accomplished by the installation of appropriately placed louvers. All fasteners for the screen or bars and louvers must be tamper-proof or tack-welded in place.

E. Locks On Perimeter Doors

When areas are not approved for classified Open Storage, and the area contains unclassified AIS, networks, and media, the systems and media must be protected from pilfering. Office doors, laboratory doors, and building perimeter doors must always be locked when the system area is left unattended and also after hours.

F. Access List

Restricted Areas approved for classified processing, must have a posted Access List to identify authorized personnel into the area during classified or sensitive unclassified processing, IAW Appendix J of OPNAVINST 5239.1A.

G. Roving Guard

A Roving Guard is provided by the Command to patrol all areas within the perimeter. The Roving Guard also provides backup and relief to other Guards and Guard posts.

H. Report Open Storage Intrusions

In event of an unauthorized penetration (access) into an Open Storage Area during normal work hours that the Open Storage area is in access, personnel must immediately notify Physical Security Group of the unauthorized penetration.

I. Cipher Locks and Card Key Systems

Cipher locks and Card Key Systems may be used as discretionary access control devices for areas approved as Open Storage areas. However, Cipher locks and Card Key Systems must not be used as the primary locking .evices used on Open Storage areas.

J. 3-Dot Key Lock

The 3-Dot key lock system at NRaD, is a special key lock distribution system. Use of this keying system may be requested from the Physical Security Group for use in areas that require protection of highly pilferable or high value equipment

K. Classified Open Storage Certification

Areas requiring the open storage (non-security container) of classified material, must submit a request for Open Storage to the Security Operations Coordinator. A Security Evaluation Team will be coordinated by the Security Operations Coordinator, and an evaluation performed at the proposed open storage site. The inspection will assess information, personnel, industrial, AIS security, physical security, and foreign disclosure

security. After passing the evaluation, all deficiencies corrected, and a written Open Storage Certification issued by the Security Operations Coordinator, the custodian for an open storage area must ensure integrity of the area at all times. The Open Storage Certification must be kept current by the custodian of the area.

L. Perimeter Fence

As part of Physical Security requirements at NRaD, a fence and natural boundaries are provided around this Naval Activity.

M. CCTV for PDS

PDS's that contain communications cables and wire with classified data transmissions (called RED data) at Top Secret and above, passing through an uncontrolled area (called Black area) to another Restricted classified area, must be physically protected by an approved PDS design, physical safeguards, and constant visual surveillance by a Closed Circuit TV (CCTV).

N. Managing Discretionary Access Control Systems

For classified open storage, restricted areas, and sensitive unclassified areas that use Discretionary Access Control Systems (i.e., cipher lock systems, card-key systems, biometrics access systems) to enhance a primary locking device (i.e., door lock, 3-Dot key lock, 3-tumbler combination lock) and to selectively authorize personnel into an area, management for the controller units must protect the controller unit from unauthorized changes and must segregate the unit from casual access by employees, contractors, and visitors.

4.2.3 Computer Security (COMPUSEC)

A. Identification & Authorization

NRaD owned and managed networks, or the host AIS and network management systems on them, must be protected with access controls that provide for the identification (i.e., User-ID) and authentication (i.e., password) of each authorized user.

B. Discretionary Access Control

NRaD owned and managed networks, and the host AIS and network management systems on them, must provide for Discretionary Access Controls (i.e., limit access to certain files and system privileges to authorized users or groups of users).

C. Object Reuse

NRaD owned and managed networks, network components and host systems on the network that process, handle, or transmit classified or sensitive unclassified data, must ensure that all residual information (i.e., residual information in buffers, cache memory, trashed printer listings, monitor screens, etc.) cannot be accessed by unauthorized users.

D. Environmental Cleanliness

All NRaD AIS and network operational environments must be kept clean and free of damaging dirt, dust, and other pollutants, and a regular cleaning schedule must be adhered to. False floor areas must be kept clean, and not used for storage purposes.

E. Environmental Detection

All NRaD AIS and networks that operate in an AIS facility or facilities, must be protected by written procedures that address Environmental controls, and by active environment protection devices that include: Heat detection sensors, smoke detectors, water sensors, water drains, humidity gauges, air conditioning, emergency power-off switches, plastic covers, Uninterruptable power supply (UPS), approved fire protection systems or equipment, and removal of excess unused wire under floor.

F. Audit of Host AIS

All NRaD AIS that process, handle, or transmit classified or sensitive unclassified data, must have an audit of system usage by a manual audit, automated audit, or combination of manual or automated audit. Single user microcomputers in locked, single occupant offices are exempt from audit of the system.

G. Regular Review of System Audit

Each NRaD AIS with system audit capability, must periodically be reviewed for compliance with access control policy of the AIS being accessed. The System manager, supervisor, or project manager must provide periodic review of the audit trail. Recommend daily review be provided at a minimum.

H. Configuration Management

NRaD owned and managed AIS and networks that process or transmit classified or sensitive unclassified data, must provide both hardware and software configuration management to ensure data integrity during equipment operation, remote connectivity, and to ensure TEMPEST controls. Software configuration management must ensure the integrity of operating system software and application programs.

I. AIS and AIS Media Declassification Procedures

All AIS and AIS media used with classified data at NRaD, or used with any AIS that has connectivity to NRaD owned and managed networks, must be proper declassified prior to using or releasing it as declassified. At NRaD, the proper ADP Security Officer (ADPSO) declassification procedure must be followed, and the appropriate DADPSSO's written certification of the declassification must be obtained, to officially declassify any system or AIS media at NRaD.

J. Risk Analysis

All AIS and networks that process or transmit classified or sensitive unclassified data, must ensure an official Risk Analysis has been performed to meet AIS security accreditation requirements required by SECNAVINST 5239.2 and OPNAVINST 5239.1A. Contact the cognizant DADPSSO for an AIS or network, to ascertain the appropriate type of Risk Analysis.

K. Security Test & Evaluation (ST&E)

As part of the Navy's AIS Security accreditation requirements, all NRaD AIS and networks that process or transmit classified or sensitive unclassified data must have an ST&E Plan developed and tested against each AIS, facility, or network handling classified or sensitive unclassified data, to ascertain the overall effectiveness of installed AIS security safeguards and countermeasures identified in the Risk Analysis.

L. Software Security & Integrity

To ensure the security and integrity of any software used at NRaD, especially for host systems with multiple users and remote network connectivity, the management for host systems must ensure that periodic security software programs (such as COPS for UNIX operated systems, or SPI for VMS operated systems) are run on the system to identify security deficiencies that require patching, and the patches made. Likewise, Network Management must ensure that network security software tools are run against host systems on the network, and that any deficiencies are identified and patches made.

M. AIS Accreditation

Department of the Navy and CO, NRaD requires all AIS and networks that are to operate with any type of data at NRaD or on behalf of CO NRaD, to first be accredited for operation after meeting all Navy and local security requirements. After the NRaD ADPSO has certified that all security requirements have been met to satisfy the Designated Approving Authority (DAA), a written authority to operate will be issued to the system or network management requesting accreditation.

N. Network Accreditation

Each major multi-organizational network at NRaD, or networks with off-center remote access controlled or managed under CO NRaD, must first obtain security accreditation to operate from the Designated Approving Authority for the overall network. Each host system on an NRaD network must be accredited, in writing, to operate and the NSO must be provided written proof of the accreditation prior to the system being granted network access. For networks managed by other than CO, NRaD, these networks must be accredited under the DAA identified by the network management. Joint service networks must be accredited concurrently by a DAA identified by network management.

O. Contingency Planning

As part of AIS security accreditation requirements, administrators of AIS or NRaD controlled networks, must ascertain if unplanned disruption of services caused by loss of system or network usage, would have critical impact on mission accomplishment. If the answer is "yes", a formal Contingency Plan is necessary and approval to develop such a

plan must be obtained. Formal written request to develop a Contingency Plan must be forwarded to NRaD ADPSO for submittal to the NRaD Information System Council (ISC), who will make final decision to approve or disapprove developing such a plan.

P. Network Security Officer (NSO)

At NRaD, each major multi-organizational network and networks, with off-center remote access, controlled or managed under CO NRaD, must have an NSO, appointed in writing, to establish written security policy, ensure compliance with network security policy, act as security point-of-contact on the network and between host sites, and investigate security incidents.

Q. Terminal Area Security Officers (TASO's)

TASO's must be appointed, in writing, at remote network sites where formal security personnel (i.e., ADP Security Officer or ADP Systems Security Officers, system management, facility management) have not been assigned. TASO's must ensure compliance with written network security policy at remote sites, and report incidents to the Network Security Officer.

R. Memorandum of Agreement (MOA)

For NRaD managed and controlled networks that will be accessed by remote site AIS at other Navy activities, contractor sites, or other agencies, a formal written and signed MOA must be established between senior officials to establish security policy and procedure to be followed in event of a security incident.

S. Backdoor Network Access

For NRaD managed and controlled networks that have been accredited to operate, all backdoor network access (i.e., backdoor access is when a new AIS or network wishes to make connectivity with an existing host AIS already accredited to operate on an existing network) will first require written proof of AIS accreditation for the AIS requiring network access, and it must be ensure all network security policy will be complied with by the backdoor AIS or network.

T. Network Configuration Diagrams

To provide integrity for networks handling or transmitting classified or sensitive unclassified data, an up-to-date configuration diagram must be maintained. Such a diagram must fully represent the actual physical layout of the network, and may be used as a tool for management to evaluate network security, and to implement required physical safeguards where required.

U. Network Connectivity Diagrams

To provide integrity for networks handling or transmitting classified or sensitive unclassified data, an up-to-date connectivity diagram must be maintained. Such a diagram must fully represent the actual logical connectivity for the network, and may be used as a tool for management to evaluate network security, and implement safeguards where required.

V. AIS Security Training

As part of NRaD's overall AIS security awareness, all personnel at NRaD must receive periodic security training. NRaD ADPSO provides periodic ADP security training to all Division ADP System Security Officers (DADPSSO's). DADPSSO's must periodically provide AIS Security Training to personnel (government and contractors) under the DADPSSO's cognizance. A yearly security training session by the Security Office must be attended by all personnel. NRaD management and supervisors must ensure personnel receive sufficient security training to meet security duties assigned to personnel. All new personnel are provided Security Awareness and OPSEC Awareness training. Numerous government and private sector training courses are available. The NRaD ADPSO may be contacted for sources of AIS security training.

W. Incident Reporting Procedures

To ensure good security practices during a network security incident, and afterwards for recovery, a written Incident Reporting Procedure is highly recommended. Formats for Incident Reporting Procedures are varied, contact the NRaD ADPSO for guidance.

X. Visitor Procedures for Classified Areas

To facilitate visitors (i.e., visitors without a proper clearance or a need-to-know for classified materials and information) into areas processing classified information, written procedures must address the requirement to fully sanitize the area by covering or securing all classified materials, powering down equipment where required, and providing a designated escort at all times. All employees in such classified areas must have knowledge of the sanitization procedures.

Y. Backup of Applications

Network management must ensure that backups are made of major software application programs for network systems and component equipment, and that backups are stored in a secure remote location for recovery purposes. Backups should likewise be made on host systems with network connectivity, and the backups should be securely stored.

Z. Operating System Backups

Network management must ensure that backups are made of operating system software programs for network systems and component equipment, and that backups are stored in a secure remote location for recovery purposes. Backups should likewise be made on host systems with network connectivity, and the backups should be securely stored.

AA. File Encryption

Though not a requirement, system users or system management may ensure data protection of files by encrypting all files as they are stored, and decrypting as they are used by authorized system users. NOTE: System performance will decrease from the use of encryption algorithms to store or access information.

AB. Security Operating Procedure (SOP)

When a system or network operates with a special environment, or with special caveat(s) of information (i.e., WNINTEL, NATO, NOFORN, NOCONTRACT, SIOP-ESI), a tailored Security Operating Procedure must be written to address the unique operational

requirements to be followed by all authorized users. The SOP may be added to the required Network Security Policy and Plans Handbook (NETSPPH), as an addendum.

AC. Restrict Global System Access

Only a minimal set of authorized system personnel (usually system management) must be granted global system access (also called SuperUser privilege) to properly manage the network or host systems. At times, select system maintenance personnel must use SuperUser privilege to accomplish their duties. During these times, the maintenance person must be continuously monitored for work performed, system changes must be documented, and the SuperUser privilege must be immediately removed upon completion of maintenance work. For classified and sensitive unclassified systems, an AIS's operating system software must be verified against a master copy of the operating system, to ensure its integrity after changes are made in equipment configuration.

AD. Equipment Configuration Management

For classified systems and network components, ensure a rigid equipment configuration control is maintained to ensure a certifiable security posture and to maintain TEMPEST certification approval for the equipment.

AE. Meets Trusted System Evaluation Criteria

All AIS, networks, or other resources must follow the "least privilege" principle defined in DoD 5200.28-STD (DoD Trusted Computer System Evaluation Criteria).

4.2.4 Communications Security (COMSEC)

A. Encryption

For classified and sensitive unclassified data transmissions into or through uncontrolled areas, transmissions must be encrypted by Navy approved encryption devices. A Communications Security Material System (CMS) encryption devices may be used; STU- III's may be used to accomplish encryption, dependent on application of the network and systems. Wireless networks transmitting classified or sensitive unclassified data must also use proper encryption for the classification or sensitivity of data to be transmitted.

B. CMS Equipment Protection

All equipment under CMS Inventory controls, must be protected in accordance with Communications Security Policy - 1 (CSP-1) and other guidelines.

C. CMS Keying Material

All keying material (keymat) protected under CMS inventory, must be protected in accordance with Communications Security Policy - 1 (CSP-1) and other guidelines.

D. Two-Person-Integrity (TPI)

TPI is a CMS requirement for handling, protecting, accountability of CMS keying materials. Mishandling of CMS material requiring TPI, carries stringent disciplinary action.

E. Cryptographic Clearance for CMS Material

All personnel and contractors that require access to CMS material in performance of their duties, must have a current clearance for General Service (GENSER) data (also called Collateral data) for the highest classification to be worked with. In addition, personnel and contractors who must have direct access to cryptographic material for their duties, must first be cleared for cryptographic material access by Director, Communications Security Material System (DCMS), prior to being granted CMS access. Prior to granting access, the Defense Investigative Service (DIS) may have additional requirements for contractor's request to access CMS material. All questions concerning CMS must be directed to the NRaD CMS Custodian.

F. CMS Inventory

All cryptographic material under control of the Communications Security Material System (CMS) are required to be inventoried by the NRaD CMS custodian on a regular basis. Mishandling of CMS inventory material carries stringent disciplinary action.

G. Protected Distribution System (PDS)

All classified data transmissions on communications lines (i.e., wire or fiber-optics) through uncontrolled areas, or areas controlled by other organizations without need-to-know, must be protected by approved PDS designs and certified locally by the NRaD TCO, if operated at Secret, and below . PDS's to be operated at Top Secret must be certified

for design and for TEMPEST requirements by a higher authority other than the TCO, prior to its implementation and operation.

H. Distribution System (DS)

All classified data transmissions at Secret, and below, on communications lines (i.e., wire or fiber-optics) through areas controlled within the same building, that contain the same classification, but are controlled by another organization without need-to-know, then the cables must be protected by hardened conduit through such areas.

I. STU-III's as CCI

Secure Telephone Units/Third Generation (STU-III's) and their Cryptographic Ignition Key (CIK), are Controlled Cryptographic Items (CCI), and must be periodically inventoried. A STU-III with it's CIK are considered classified CCI when used with each other. Classified CIK's must be stored in security containers, or approved classified open storage areas, when not being used or taken home.

J. STU-III's Used With AIS or FAX

A STU-III may be approved to transmit varied encrypted classified, or sensitive unclassified data, over public phone lines (a phone network), when the STU-III is to be used with AIS's or with a Navy-approved Facsimile (FAX) machine. The NRaD STU-III Manager is responsible for ensuring the STU-III installation requirements are met. Additionally, STU-III's must be approved for use with an AIS or FAX, when the AIS or FAX is initially installed, and upon removal of such equipment.

STU-III and AIS Accreditation: For STU-III's that are to be operated with an AIS, a written AIS security accreditation must be obtained for the location of operation, by contacting the cognizant DADPSSO for submittal of required accreditation documents to the NRaD ADPSO.

STU-III/FAX Approval: For STU-III/FAX machine approval, contact the DADPSSO to submit required documentation for requesting written approval to operate, and to obtain required Security Operating Procedures.

AIS accreditation or STU-III/FAX approval must be granted in writing prior to operating a STU-III with peripheral equipment, and before operating equipment that has been moved from its approved site.

When a STU-III is not being used for classified data transmission, but is located near equipment or AIS processing classified data, RED-to-BLACK separation requirements must be followed, as stated below in the EMANATIONS SECURITY section.

K. Communications with Contractor Facilities

When contractor support for NRaD involves communications between the contractor facility and NRaD, the Defense Investigative Service (DIS) must first approve the contractors connectivity in accordance with Defense Industrial Security requirements, and a written Memorandum of Agreement (MOA) is required, must be established between the contractor facility and Commanding Officer, NRaD, to identify security responsibilities. Additionally, the NRaD AIS, and its connectivity to the contractor facility, must be accredited to operate (in writing) by the appropriate DAA.

L. Peer Authentication

For classified or sensitive unclassified communication links between two or more remote points, the originator of the link must obtain Peer authentication from each remote point (its Peer) being accessed, to ensure authentication that the same classification or sensitive of data may be transmitted to that remote point. Methods for Peer Authentication are varied in accordance with the type of technology being used. In the case of STU-III's, voice recognition of the remote user's voice may suffice along with the required STU-III LED panel that shows name of remote site, and the highest authorized classification level to be handled or discussed. Varied authentication techniques, software, and firmware programs may be implemented as part of a "Peer Authentication". Suggest that DoD 5200.28-STD, the "Orange Book" be obtained for further guidance on "Peer Authentication".

4.2.5 Emanations Security

A. RED-to-BLACK Separation Requirements

As part of the Navy's promulgation of the National Policy on control of compromising emanations, RED-to-BLACK separation is summarily the requirement to physically keep classified (RED) electronic equipment and cables separated from all unclassified (BLACK) electronic equipment and cables by a set distance criteria to control compromising emanations. At NRaD, the RED-to-BLACK minimum separation requirement is 1 meter (3 feet).

Fiber Optics

Because of the noise-immunity and non-emission characteristics of fiber-optic cables, multiple levels of data can be transmitted over different fibers within the same cable, or within different cables that are within the one meter separation limit, under the following conditions:

- Fiber cables shall be physically protected to the highest level of data being transmitted. That is, if the highest level of classification of data being transmitted on a network fiber is SECRET, then the entire length of the cable must be protected as a SECRET asset.
- Fiber cables shall be constructed of all-dielectric (non-electrical conducting) materials (i.e., no metal allowed in the construction of the cable including; strength members, shields, copper wire composites, etc.)
- Termination devices connected to the fibers (i.e., fiber-optic transceivers, fiber-optic repeaters, etc.) shall meet the one meter separation for containing data at different classification levels.
- All node devices (i.e., hosts, repeaters, routers, bridges, etc.) shall meet the one meter separation for networks containing data at different classification levels.
- All fiber-optic connections and runs shall be under configuration control, and all fiber-optic interfaces shall be labeled as to the highest data classification allowed on that device (e.g., both ends of a fiber jumper cable from a patch panel to the optical device will be labeled - the fiber-optic cable connecting to the back of the patch panel would not).

B. TEMPEST Visual

The NRaD TCO must provide a TEMPEST Visual to all electronic equipment and systems planning to handle, process, or transmit classified information, and all TCO identified TEMPEST vulnerabilities must be corrected, prior to actual classified operation of the electronic equipment.

C. TEMPEST Shielded Enclosures

Although such enclosures are not a requirement for classified processing environments, certain designated areas, buildings, and containers at NRaD (specially constructed to meet TEMPEST Shielded Enclosure criteria) are to be used as TEMPEST

Shielded Enclosures. Prior to a TEMPEST Shielded Enclosure, or TEMPEST Shielded building being used for classified processing, the enclosure, building, or container must be certified by a TEMPEST certifying authority. TEMPEST shielded enclosure certifications must be kept current by following set procedures, performing regular shield maintenance, facility manager(s) maintaining the integrity of the shield, and periodic Instrumented TEMPEST test. Contact the NRaD TCO to ascertain how to obtain TEMPEST certification for a Shielded Enclosure, Shielded Building, or Shielded Container.

D. Filters for TEMPEST Shielded Areas

At NRaD, areas that are TEMPEST certified (i.e., Shielded Enclosures, Shielded Building, and Shielded Containers) must have filters on all phone lines, communication lines, and power lines that ingress and egress the shielded enclosure. Wave-guide filters must be used for fiber-optic cables entering and exiting the shielded enclosure.

E. Protected Distribution System (PDS) Certification

As discussed in the COMMUNICATIONS SECURITY (COMSEC) section, PDS must be approved for their design prior to implementation, and PDS must be reviewed, for Secret, and below, by the NRaD TCO. For a PDS to be operated at Top Secret, the PDS must be certified for design and for TEMPEST, prior to implementing the PDS; these PDS's must be certified by higher authority beyond NRaD.

F. Distribution System (DS) Certification

Distribution Systems with classified data transmissions at Secret, and below, through areas containing the same classification, but controlled by another organization without need-to-know, then the cables in the DS must be protected by hardened conduit. If transmitted data is Secret, and below, the DS may be certified locally by the NRaD TCO. If a DS is to be operated at Top Secret, it must be certified for design and for TEMPEST requirements by higher authority, prior to its implementation and operation.

G. Shielded Enclosure Maintenance Program

For NRaD areas certified as TEMPEST Shielded Enclosures, the enclosure must have a designated Facility Manager to ensure required regular maintenance of the enclosure and to ensure the enclosures integrity. The NRaD TCO may be contacted to ascertain full Shielded Enclosure Maintenance Program requirements.

H. RED-to-BLACK Trays for Cables

To ensure RED-to-BLACK TEMPEST separation requirements and control of compromising emanations in larger AIS facilities, and office areas with numerous AIS, it is recommended that tray runs with RED (i.e., classified) cable and wire be implemented in classified processing areas (or areas with various types of electronic equipment), and the RED trays, separated by 1 meter (3 feet) from tray runs of BLACK (i.e., unclassified) lines and cables in the same classified processing area. Separation of cables is recommended in shielded enclosures to ensure control of compromising emanations and integrity of configuration management.

I. Separation of Power Source

TEMPEST guidance recommends that electronic equipment used for processing, handling, or transmitting classified data, be provided with a separate power source (i.e., separate circuits or power panels) than is provided for electronic equipment used for processing, handling, or transmitting unclassified data.

J. Good Housekeeping in Classified Facilities

To ensure good RED-to-BLACK separation requirements, Facility Managers must ensure all old or unused cables and wires are removed from facilities that electronically process or transmit classified information.

NOTE:
This is also a good procedure to reduce the risk of fire in false-floor areas of a facility!

K. Grounding of TEMPEST Shielded Enclosures

At NRaD, for all areas certified as TEMPEST Shielded Enclosures, the facility manager must ensure the integrity of the Shielded Enclosure grounding at all times.

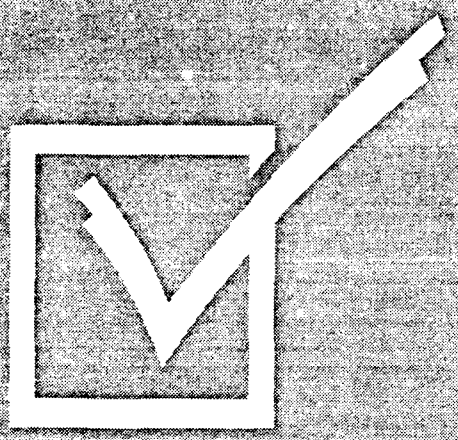
L. Public Address (PA) Systems

At NRaD, in areas to be used as classified AIS facilities, installation of public address or intercom systems are not authorized. If one is installed, it is treated as a network; RED-to-BLACK separation requirements must be adhered by ensuring that the integrity of classified information within such a facility is maintained.

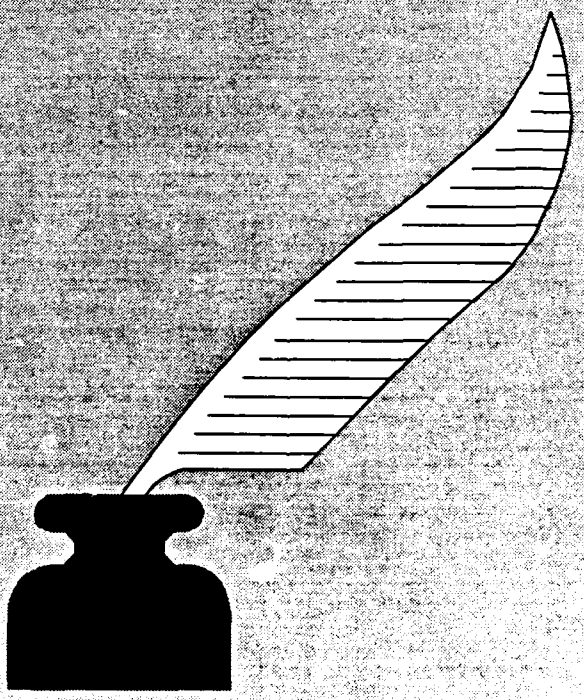
4.3 Projects, Programs, and Special Considerations

4.3.1 Multi-Level Security (MLS)

Multi-Level Security networks (either commercially available or currently under development) are designed with security considerations and with the intent to allow trusted network management systems and trusted software to disseminate varied concurrent classified, and unclassified data levels, to authorized remote node users. Based upon proper security clearances (i.e., authorization, need-to-know, physical security, communications security, information and personnel security, configuration management, and security operating procedures) MLS must be tightly controlled. At this time MLS must be approved by a DAA beyond CO, NRaD. Special requests and documentation must be developed to request DAA approval via NRaD ADPSO.



APPENDIX



APPENDIX A

INDUSTRIAL SECURITY REQUIREMENTS

Classified information may be disclosed to DoD contractors cleared under the Industrial Security Regulation. Release of information on NRaD networks, both classified and unclassified, to contractor personnel must be accomplished under an existing contract. Contractual restrictions are placed on contractor personnel, limiting the classification of the material they may access, as well as other special categories of information. The following categories, and their specific restrictions, apply to contractor use of NRaD networks, and the access authorization which must be given on the contractor's Contract Security Classification Specification (DD Form 254), attached to their contract.

Because of the difficulty in protecting information located on a computer network, your DADPSSO should be brought into the picture at the beginning of a contract. All information, both classified and unclassified, located on the network may be releasable to the contractor at the level found on the contract DD Form 254, or be protected from release using approved methods. The DD Form 254 must also include all special categories you require your contractor to access on your network.

Extreme caution must be taken to ensure that special categories of information, unclassified or classified, are not inadvertently divulged to contract personnel who do not have the need-to-know established by a current contract DD Form 254. Approved methods to protect the following categories of information are available from your DADPSSO. The following special categories, and their specific restrictions pertinent to contract personnel, must be identified on each network and protected from inadvertent access by contract personnel.

NATO

This means information belonging to, and circulated by, the North Atlantic Treaty Organization (NATO). Access to NATO information by contractor personnel requires a final U.S. Government clearance at the appropriate level and special briefings. Extreme caution must be used if NATO information is on your network.

FOREIGN GOVERNMENT INFORMATION

FOREIGN GOVERNMENT INFORMATION is information that is provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

Produced by the United States pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

This includes any FOREIGN GOVERNMENT INFORMATION, except NATO. Access to FOREIGN GOVERNMENT INFORMATION requires a final U.S. Government clearance at the appropriate level. Extreme caution must be maintained if FOREIGN GOVERNMENT INFORMATION is on your network. This information has been entrusted to the United States, and we have accepted it promising the originating country non-disclosure to a third party. Failure on NRaD part to properly protect FOREIGN GOVERNMENT INFORMATION must be reported to the Navy International Programs Office (IPO), who will in turn notify the originating country.

INTELLIGENCE INFORMATION

This is information under the jurisdiction and control of the Director of Central Intelligence (DCI) and circulated within the Intelligence Community. The term INTELLIGENCE means foreign intelligence and counterintelligence and information describing U.S. foreign intelligence and counterintelligence activities, sources or methods, equipment, and methodology used for the acquisition, processing, or exploitation of intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from U.S. collection efforts.

DoD contractors may be provided selected intelligence when required in the performance of a Department of the Navy contract unless specifically prohibited. Authorization for release of intelligence to a contractor in the performance of a specific contract in no way implies authorization for release under another contract.

INTELLIGENCE INFORMATION will be released on a strict need-to-know basis. Access to INTELLIGENCE INFORMATION requires a final U.S. Government clearance at the appropriate level.

You must ensure that contractor personnel will NOT:

- reproduce INTELLIGENCE INFORMATION, except for further Government use;
- release INTELLIGENCE INFORMATION to foreign nationals or immigrant aliens regardless of their security clearance;
- release INTELLIGENCE INFORMATION to an employee not directly involved in the performance of the specific contract, or;
- release INTELLIGENCE INFORMATION to another contractor, Government agency, private individual or organization.

DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON)

This marking is used so the originator will have continuing knowledge and supervision of the use made of the information. Information bearing this marking may not be incorporated in whole or in part into an NRaD network without the advance permission of and under conditions specified by the originator. All ORCON material must be approved for release prior to dissemination to contract personnel. Any ORCON information on NRaD networks must be protected from inadvertent access by contract personnel.

Markings on source material may include, but not be limited to, "ORCON" or "OC".

NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (NOCONTRACT)

This marking is used to prohibit the dissemination of information to contractors/consultants without the permission of the originator. This marking is used only on INTELLIGENCE INFORMATION which, if disclosed to a contractor or consultant, would actually or potentially give him or her a competitive advantage which could reasonably be expected to cause a conflict of interest with the obligation to maintain the security of the information, or which was provided by a source on the express or implied condition that it not be made available to contractors/consultants.

NRaD networks containing source material marked NOT RELEASABLE TO CONTRACTORS/CONSULTANTS may not be accessed by either contractors or consultants. These restrictions do not apply to consultants hired by NRaD under Office of Personnel Management and who are considered to be extensions of NRaD.

Markings on source material may include, but not be limited to, "NOCONTRACT" or "NC".

CAUTION-PROPRIETARY INFORMATION INVOLVED (PROPIN)

This marking is used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data believed to have actual or potential value. Information bearing this marking will not be disseminated in any form without the permission of the originator to an individual, organization, or foreign government which has any interests, actual or potential, in competition with the source of the information.

This marking may be used in conjunction with the "NOCONTRACT" marking to preclude dissemination to any contractor. The short form of this marking is "PROPIN"; the abbreviated form is "PR".

RESTRICTED DATA (RD)

This is information which is classified and controlled under the Atomic Energy Act of 1954. RESTRICTED DATA information covers:

- Design, manufacture or utilization of atomic weapons;
- The production of special nuclear material;
- The use of special nuclear material in the production of energy, but not to include data declassified and removed from the Restricted Data category under Section 142 of the Atomic Energy Act (see Formerly Restricted Data).

Access to RESTRICTED DATA requires a final U.S. Government clearance at the appropriate level.

FORMERLY RESTRICTED DATA (FRD)

FORMERLY RESTRICTED DATA is information removed from the RESTRICTED DATA category upon determination jointly by the Atomic Energy Commission and Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. Such information is, however, treated the same as RESTRICTED DATA for purposes of foreign dissemination.

Caution must be taken when giving access to this information. Although it is FORMERLY RESTRICTED DATA, it is sensitive in nature. Consult with your DADPSSO prior to allowing contract personnel access to FORMERLY RESTRICTED DATA information.

CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)

CNWDI is Restricted Data revealing the theory of operation or design of the components of a thermonuclear implosion type fission bomb, warhead, demolition munitions or test device. Specifically excluded is information concerning arming, fusing and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among those excluded items are the components which personnel set, maintain, operate, test or replace.

Markings on your source material may include, but not be limited to, "CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION", "CNWDI", or "N".

Any CNWDI information contained on your network must be protected from disclosure to contract personnel. Special briefings and procedures are required. Access to CNWDI requires a final U.S. Government clearance at the appropriate level.

LIMITED DISSEMINATION (LIMDIS)

LIMDIS means restrictive controls established by an original classification authority to emphasize need-to-know protective measures available within the regular security system. Contract personnel may be granted access to specific programs subject to LIMDIS controls, by program name. This authorization must be specific on the DD Form 254, to include the program name.

FOR OFFICIAL USE ONLY (FOUO)

FOR OFFICIAL USE ONLY is information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552.

Any FOR OFFICIAL USE ONLY data on your network must be protected from inadvertent disclosure to contract personnel.

FOR OFFICIAL USE ONLY information must be safeguarded by the contractor as specified in Chapter 13, Section 6, Industrial Security Manual.

COMMUNICATIONS SECURITY (COMSEC) INFORMATION

COMMUNICATIONS SECURITY are the protective measures taken to deny unauthorized persons access to information derived from telecommunications of the U.S.

Government related to national security and to ensure the authenticity of such communications.

COMSEC information includes accountable, or non-accountable, COMSEC information and controlled cryptographic items. Contractor access to any COMSEC information requires special briefings at the contractor facility. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level.

APPENDIX B

FOREIGN DISCLOSURE REQUIREMENTS

Releasing information, classified or unclassified, to a representative of a foreign government must be strictly controlled. Release of information to a representative of a foreign government, including U.S. citizens employed by that government, requires approval from the Navy International Programs Office (Navy IPO). Navy IPO receives requests directly from foreign countries, requests NRaD recommendation for release of the information, then makes the final determination based on input from this Division, as well as the sponsoring command. It is therefore imperative that no information, either classified or unclassified, be made available to a foreign representative prior to approval of the Navy IPO.

Because of the difficulty in protecting information located on a computer network, your DADPSSO and the Foreign Disclosure Officer (FDO) must coordinate this effort. All information, both classified and unclassified, located on the network must be either releasable to the country in question, or be protected from release using approved methods.

Your DADPSSO will require a listing of all information on the network, and your proposed plan to protect this information, to pass to the FDO. If your network contains information that has not been authorized for release to the country in question, then the FDO will submit a request to Navy IPO for release.

Extreme caution must be taken to ensure that special categories of information, unclassified or classified, are not inadvertently divulged to foreign nationals. Approved methods to protect the following categories of information are available from your DADPSSO. The following special categories, and their specific restrictions pertinent to foreign nationals, must be identified on each network and protected from access by foreign nationals.

NATO

This means information belonging to, and circulated by, the North Atlantic Treaty Organization (NATO). Access to NATO information by foreign nationals is restricted to citizens of NATO member nations. Visitors from NATO countries are NOT automatically eligible for access to NATO information. For NATO information in NRaD possession, access is authorized based on their specific purpose of visit, their need-to-know, the

releasability to their country, and the approval of Navy IPO. Extreme caution must be used if NATO information is on your network.

FOREIGN GOVERNMENT INFORMATION

FOREIGN GOVERNMENT INFORMATION is information that is provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or produced by the United States pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

This includes any FOREIGN GOVERNMENT INFORMATION, except NATO. Access to FOREIGN GOVERNMENT INFORMATION, in the possession of NRaD, requires the specific approval of the Navy IPO. Extreme caution must be maintained if FOREIGN GOVERNMENT INFORMATION is on your network. This information has been entrusted to the United States, and we have accepted it promising the originating country non-disclosure to a third party. Failure on NRaD's. part to properly protect FOREIGN GOVERNMENT INFORMATION must be reported to the Navy IPO, who will in turn notify the originating country.

INTELLIGENCE INFORMATION

This is information under the jurisdiction and control of the Director of Central Intelligence (DCI) and circulated within the Intelligence Community. The term INTELLIGENCE means foreign intelligence and counterintelligence and information describing U.S. foreign intelligence and counterintelligence activities, sources or methods, equipment, and methodology used for the acquisition, processing, or exploitation of intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from U.S. collection efforts.

Classified INTELLIGENCE INFORMATION, even though it bears no control markings, will not be released in any form to foreign nationals, or immigrant aliens (including U.S. Government employed, utilized or integrated foreign nationals and immigrant aliens) without permission of the originator.

Release of classified INTELLIGENCE INFORMATION to a foreign company under contract to the U.S. Government will be made through the government under which the company operates.

Direct U.S.-to-foreign contractor release is prohibited.

Classified INTELLIGENCE INFORMATION originated within the Department of Defense (DoD) and not bearing any control markings may be released to foreign governments if the release is authorized by proper authority. Classified INTELLIGENCE INFORMATION originated by non-DoD members of the Intelligence Community not bearing any of the control markings may be extracted or paraphrased and used by Department of the Navy commands in information disseminated to foreign governments (except when categorized as Restricted Data and Formerly Restricted Data) provided:

No reference is made to the source documents upon which the released product is based.

The information is extracted or paraphrased in such a way that the source or manner of acquisition of the intelligence cannot be deduced and is not revealed in any manner.

Foreign release is made through established foreign disclosure channels and procedures.

Markings on source material may include, but not be limited to, "Intelligence Sources or Methods Involved", "WNINTEL", or "WN".

If there is any doubt that INTELLIGENCE INFORMATION is contained in your network, do not grant access to the network to foreign nationals. Contact your DADPSSO and the FDO for further assistance.

DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON)

This marking is used so the originator will have continuing knowledge and supervision of the use made of the information. Information bearing this marking may not be incorporated in whole or in part into an NRaD network without the advance permission of and under conditions specified by the originator. All ORCON material must be approved for release prior to dissemination to foreign nationals. Any ORCON information on NRaD networks must be protected from inadvertent access by foreign nationals.

Markings on source material may include, but not be limited to, "ORCON" or "OC".

AUTHORIZED FOR RELEASE TO (NAME OF COUNTRY/INTERNATIONAL ORGANIZATION)

This marking is used to identify classified intelligence that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign country(ies)/organization(s) indicated. No other foreign dissemination of the material is authorized without the permission of the originator. This marking may be abbreviated "REL TO (abbreviated name of country(ies)/organization)."

If any information is on your network with this marking, notify the DADPSSO and the FDO prior to giving access.

NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN)

This identifies intelligence that may not be released in any form to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator. This marking is used on intelligence which, if released to a foreign government or national, could jeopardize intelligence sources or methods, or which would not be in the best interests of the United States to release from a policy standpoint, as specifically determined by a Senior Official of the Intelligence Community.

Markings on source material may include, "NOT RELEASABLE TO FOREIGN NATIONALS", "NOFORN" or "NF". Contact your DADPSSO and the FDO for further assistance.

CAUTION-PROPRIETARY INFORMATION INVOLVED (PROPIN)

This marking is used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data believed to have actual or potential value. Information bearing this marking will not be disseminated in any form without the permission of the originator to an individual, organization, or foreign government which has any interests, actual or potential, in competition with the source of the information. This marking may be used in conjunction with the "NOCONTRACT" marking to preclude dissemination to any contractor.

The short form of this marking is "PROPIN"; the abbreviated form is "PR".

RESTRICTED DATA (RD)

This is information which is classified and controlled under the Atomic Energy Act of 1954. RESTRICTED DATA information covers:

- Design, manufacture or utilization of atomic weapons;
- The production of special nuclear material;
- The use of special nuclear material in the production of energy, but not to include data declassified and removed from the Restricted Data category under Section 142 of the Atomic Energy Act (see Formerly Restricted Data).

- Access to RESTRICTED DATA by foreign nationals is prohibited.

Contact your DADPSSO and the FDO for further assistance.

FORMERLY RESTRICTED DATA (FRD)

FORMERLY RESTRICTED DATA is information removed from the RESTRICTED DATA category upon determination jointly by the Atomic Energy Commission and Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. Such information is, however, treated the same as RESTRICTED DATA for purposes of foreign dissemination.

CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI)

CNWDI is Restricted Data revealing the theory of operation or design of the components of a thermonuclear implosion type fission bomb, warhead, demolition munitions or test device. Specifically excluded is information concerning arming, fusing and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among those excluded items are the components which personnel set, maintain, operate, test or replace.

Markings on your source material may include, but not be limited to "CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION", "CNWDI", or "N".

Any CNWDI information contained on your network must be protected from disclosure to foreign nationals.

LIMITED DISSEMINATION (LIMDIS)

LIMDIS means restrictive controls established by an original classification authority to emphasize need-to-know protective measures available within the regular security system.

Navy IPO must authorize foreign nationals to have access to program information subject to LIMDIS controls.

FOR OFFICIAL USE ONLY (FOUO)

FOR OFFICIAL USE ONLY is information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552.

FOR OFFICIAL USE ONLY information may not be released to foreign nationals without approval of Navy IPO. Any FOR OFFICIAL USE ONLY data on your network must be protected from disclosure to foreign nationals.

COMMUNICATIONS SECURITY (COMSEC) INFORMATION

COMMUNICATIONS SECURITY are the protective measures taken to deny unauthorized persons access to information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. COMSEC information includes accountable, or non-accountable, COMSEC information and controlled cryptographic items.

Access to COMMUNICATIONS SECURITY is not authorized to foreign nationals; therefore, network access to COMSEC information must be denied.

APPENDIX C

NRAD NETWORK SECURITY POINTS-OF-CONTACT

TITLE	NAME	PHONE NUMBER*
NRaD Center Duty Officer (24 hrs/day)	Varies	(619) 553-4621
Head, Security Office Code 035	Richard Fletcher	(619) 553-3150
Infor., Personnel, and Operations, Security Group, Code 0352	R. Paller	(619) 553-3194
Operations Security (OPSEC) Code 0352	Bert Jackson	(619) 553-3005
Electronic Systems Security Group, Code 0353	M.J. Ferro-Czech	(619) 553-3186
NRaD ADP Security Officer (ADPSO), Code 0353	M.J. Ferro-Czech	(619) 553-3186
NRaD TEMPEST Control Officer (TCO), Code 0353	Rick Avila	(619) 553-5287
NRaD CMS Custodian Code 03531	LT A. Swalla,USN	(619) 553-5066
NRaD STU-III Manager Code 03532	Maggie Minor	(619) 553-4740
Physical Security Group, Code 0354	Thomas Slaughter	(619) 553-4615
ID/Access Admin. Services Section, Code 03541	W. Montgomery	(619) 553-3203
NRaD Network Security Manager, Code_____	Vacant	(Contact ADPSO)
NRaD Major Network Security Officers (NSO's):		
SWAN NSO, Code 0292	Don Schirr	(619) 553-6354
GCB NSO, Code 0293	Ty Wernet	(619) 553-2281
ADSI NSO, Code 432	Kevin Boner	(619) 553-3558

* For NRaD DSN's, drop area code which is in parenthesis.

APPENDIX D
FORMS AND NETWORK ADMINISTRATORS TOOLS

TABLE OF CONTENTS

AIS SECURITY IDENTIFICATION FORM (SIF)

Date:

From: DADPSSO, Code _____
Name _____
To: Code 0353

1. SYSTEM IDENTIFICATION *(CPU/MAINFRAME).*

a. System Name: _____
b. SIN # _____
c. Manufacturer:_____
d. Bar Code # _____
e. Model: _____
f. Serial # _____
g. Location: Bldg. ___ Room ___ Site __ (TS,BS,SS,HI,CS,PA,LA)
h. Primary User: _____ Code ____ Phone _____
i. Custodian: _____ Code ____ Phone _____

2. SYSTEM INFORMATION

( ) Single User System ( ) Shared, Single User System
( ) Host System, Multiple Users

All system/network users:

Are cleared for highest security classification of data:Y/N
Have need-to-know for all data stored: Y/N
System area is certified for open storage: Y/N
System is located in TEMPEST Shielded Enclosure: Y/N
System is regularly taken off-site: Y/N
System is personally owned: Y/N
System is contractor owned: Y/N
System is operated by contractor(s):Y/N Contract #_____
Operating system software & version _____
Application software & version _____

3. TYPE OF DATA PROCESSED *(CHECK ALL THAT APPLY)*

( ) TOP SECRET ( ) SECRET
( ) CONFIDENTIAL ( ) UNCLASSIFIED
( ) SENSITIVE UNCLASSIFIED (e.g., Privacy Act, FOUO, Financial, Sensitive Management)

SPECIAL ACCESS CATEGORIES:
( ) NATO ( ) INTELLIGENCE DATA
( ) NOFORN ( ) WNINTEL
( ) LIMDIS ( ) CNWDI
( ) RESTRICTED DATA ( ) FORMERLY RESTRICTED DATA
( ) FOREIGN GOVERNMENT INFORMATION. SPECIFY _____

4. NETWORK CONNECTIVITY *(CHECK ALL THAT APPLY)*

MILNET/INTERNET accessed via:
( ) TAC port ( ) Modem
( ) T-BOX ( ) Ethernet Cable

( ) Facsimile Connection ( ) SACS Connection
( ) NRaD Host NRaD GCB accessed via:_____
( ) Network, _____ nodes, _____ terminals, _____ server
( ) CATS (Telephone) System connection
( ) Cellular telephone modem used
( ) Dial up access used to NRaD or remote computer(s)
( ) Wireless networks (Provide name) _____
( ) Other networks/LANS/PDS accessed: _____
( ) CRYPTOGRAPHIC equipment used (Provide type) _____

5. SECURITY INFORMATION ***(Items marked with "*" are mandatory requirements for classified and sensitive unclassified processing.)***

*( ) COPS security program run and reported problems fixed (UNIX only)
*( ) SPI security program run and reported problems fixed (VMS only)
*( ) System is audited by _ automation, _ manual, _ both
*( ) System displays warning message for unauthorized access (physically or electronically)
*( ) Shared peripheral equipment used with other system(s), provide bar codes of other AIS in comments section
*( ) DADPSSO has given user appropriate chapters of SPPH
*( ) Users are trained in proper security procedures
( ) Contingency plan required _____ yes, _____ no
( ) System access controlled by user-id/password
( ) Anti-viral software used, name _____ version ____
( ) System has an internal hard drive (Level I only)
( ) System uses hard disk protect program Protect.Com for DOS or LockDisk CDEV for MACs
( ) System memory is non-volatile (RAM is not purged upon loss of power)

6. PERIPHERAL EQUIPMENT ***(Required for all Level I systems and multi-user Level II systems)***

TYPE	MANUFACTURER	MODEL	BAR CODE	SERIAL NUMBER

7. COMMENTS:

_____

_____

_____

9/92

Date ___/___/___

MEMORANDUM

From: Code _____ DADPSSO
To: Code _____ Custodian Name _____
Via: Code 0353

Subj: CERTIFICATION OF DECLASSIFICATION

1. Supporting declassification information. Item 1.i should be a detailed description. AIS/media used with SECRET and above data requires two witnesses for declassification.

a. Highest level of data processed/stored: _____

b. Secret Material Bar Code and Copy #'s: _____

c. Description of material: _____

d. Equipment type: _____

e. Equipment/Component Make/Model:_____

f. Equipment/Component Serial Number: _____

g. Equipment/Component Bar Code Number: _____

h. Component is/was used with SIN number: _____

i. Specific tool/procedure used to declassify: _____

_____

_____

j. Current/future disposition: _____

We certify that the above equipment/media has been fully and correctly declassified by an NRaD ADPSO approved declassification procedure or NSA approved equipment and is totally and unequivocally unclassified.

_____ _____ _____ _____
Signature of Witness Code Telephone No. Date

_____ _____ _____ _____
Signature of Witness Code Telephone No. Date

_____ _____ _____ _____
Signature of DADPSSO Code Telephone No. Date

NOTE: Secret Material Inventory red barcode(s) must be removed from equipment/media and submitted with a copy of this certification to Code 1312. A copy of the barcode(s) should be attached to the original certification.

3/92

Page 1 of 1

Date ___/___/___

MEMORANDUM

From: Code ____ DADPSSO
To: Code 0353

Subj: TEMPEST QUESTIONNAIRE

1. The following information should be provided for all systems prior to processing GENSER Top Secret data. Area/configuration diagrams will be attached for other than single user systems.

a. General description of data being processed (e.g., MTF messages, word processing documents):

_____

b. Listing and description of equipment being used:

System nomenclature: _____

SIN number: _____

Bar code: _____

Building: _____

Room: _____

Site: _____

Is this off the shelf equipment? YES/NO

List all system/equipment components:

NOMENCLATURE	MANUFACTURER	BAR CODE	MODEL	SERIAL NUMBER

c. Volume of data and output generated:

Top Secret	_____%
Secret	_____%
Confidential	_____%
Unclassified	_____%
	100 %

d. Remarks. Include any information that could assist in determining hazard probabilities (e.g., old telephone lines in area, no cable separation, ADPE not plugged in to dedicated power outlet, etc.).: _____

_____

_____

_____

3/92

ENVIRONMENTAL AND PHYSICAL SECURITY SURVEY

Complete a survey for each area (i.e., building, laboratory, wing) where automated information systems (AIS) and network resources under your cognizance are to be used. This survey is valid for three years but must be reevaluated if major changes occur.

Code ____ Building ___ Room _____ Wing ____ Site _____

Network Name _____ Facility/Laboratory Name _____

_____ _____ _____

DEPT/DIVISION ADP SYSTEMS SECURITY OFFICER CODE DATE

_____ _____ _____

NETWORK SECURITY OFFICER CODE DATE

All buildings and facilities that house AIS and networks must meet mandatory minimum environmental and physical security requirements as defined in SECNAVINST 5239.2 and OPNAVINST 5239.1A. After each requirement, mark each control in place which is used to meet the requirement. All items marked with "*" are mandatory and must be implemented.

Taking into consideration the existing controls, estimate the value of each threat. Threat value is defined as LOW if the threat is very unlikely to occur, not applicable or it is adequately controlled by existing countermeasures. Threat value is defined as MODERATE if the threat would have a moderate impact. Threat value is defined as HIGH if the threat is likely to occur and the impact would be significant.

a. Adequate Electrical Power Service

*( ) Primary power and outlets
*( ) Emergency lighting (COMPUTER LAB)
( ) Primary lighting
( ) Power filters
( ) Voltage regulators
( ) Uninterruptable power supply (UPS)
( ) Other _____

Assessment of Risk:

( ) LOW ( ) MODERATE ( ) HIGH

b. Adequate Fire Protection

*( ) CO2/Halon fire extinguishers within 50ft of equipment
*( ) Functioning fire alarms
*( ) Training in fire evacuation procedures
*( ) Training in emergency power down procedures (COMPUTER LAB)
*( ) Smoke/heat detectors installed (COMPUTER LAB)
*( ) Emergency power-off switch (COMPUTER LAB)
( ) Under the floor fire suppression system (COMPUTER LAB)
( ) Other _____

Assessment of Risk:

( ) LOW ( ) MODERATE ( ) HIGH

c. Adequate Housekeeping

*( ) Routine cleaning schedule adhered to
*( ) Custodian or representative present during cleaning
*( ) Non-combustible waste baskets with tight fitting covers used in equipment areas (COMPUTER LAB)
*( ) Air conditioning filters cleaned regularly (COMPUTER LAB)
( ) Area under false floors are not used as storage areas (COMPUTER LAB)
( ) Steel wool buffing pads are not used (COMPUTER LAB)
( ) Floors polished with non-flake wax (COMPUTER LAB)
( ) Other _____

Assessment of Risk:

( ) LOW ( ) MODERATE ( ) HIGH

d. Proper Temperature/Humidity

( ) Equipment operated within temperature and humidity range specified by vendor
( ) Only authorized personnel operate controls
*( ) Adequate cooling and controls
*( ) Temperature recorder in use (COMPUTER LAB)
*( ) Humidity recorder in use (COMPUTER LAB)
*( ) Temperature alarm (COMPUTER LAB)
*( ) Humidity alarm (COMPUTER LAB)
( ) Other _____

Assessment of Risk:

( ) LOW ( ) MODERATE ( ) HIGH

e. Adequate Water Damage Protection

*( ) Plastic sheets readily available to cover equipment
( ) Water/steam pipes/restroom located directly above equipment
( ) Cables are provided protection from water damage
( ) Raised floor (COMPUTER LAB)
( ) Water detection devices under the floor (COMPUTER LAB)
( ) Under floor drains are installed (COMPUTER LAB)
( ) Other _____

Assessment of Risk:

( ) LOW ( ) MODERATE ( ) HIGH

f. Adequate Physical Security

*( ) Room locked when unattended
*( ) Zero key lock system in use (Base Master System)
( ) Motion detectors installed
( ) Open door detectors installed
( ) Approved vault/strongroom
( ) Restricted area signs posted
( ) Cipher door locks in use (not used as primary barrier)
( ) Combination door locks in use
( ) 3 dot key lock system in use
( ) Door hinges pinged or spot welded
( ) Opaque windows or windows covered (blinds, curtains)
( ) Intrusion Detection System (IDS) installed
( ) Protected Distribution System (PDS) constantly monitored in unsecure areas
( ) Other _____

Assessment of Risk:

( ) LOW ( ) MODERATE ( ) HIGH

g. Adequate Physical Security (Networks only)

( ) Approved Protected Distribution Systems (PDS's) for unencrypted Top Secret data transmissions through unsecure areas, are provided constant monitoring & alarm, and regular visual checks of the external PDS are made
( ) Approved PDS's for unencrypted Confidential & Secret data through unsecure areas are provided the required physical protection, and regular visual checks of the external PDS are made
( ) Each network node is provided physical security at the required security level for the entire network

( ) The network management system, controller, or server are provided physical protection/access only to authorized network managers and personnel

( ) Network cable/fiber used for classified data transmissions are continuously provided required physical protection from personnel and visitors without proper clearance or certifiable need-to-know

( ) Access to network line analyzers, bridges, hubs, routers, concentrators, multiplexers, network monitors and reflectometers are physically controlled to ensure they are not used by unauthorized personnel

( ) All locations of externally laid underground network cable/fiber are provided adequate physical protection and properly identified with warning signs

( ) Wireless network communication components are provided physical protection to ensure unauthorized changes to position and connectivity cannot be made

( ) Network encryption devices are provided required physical protection from all personnel without proper authorization to access CMS materials & equipment

Assessment of Risk:

( ) LOW ( ) MODERATE ( ) HIGH

Additional comments

_____

_____

_____

_____

_____

_____

4/92

Date ___/___/___

COMPUTER VIRUS INFECTION REPORT

1. SIN: _____ Bar Code: _____ Make/Model: _____

2. Building: _____ Room/Lab: _____ Site: ____ (TS,BS,SS,HI,CS,LA,PA)

3. Highest level of data processed: _____

4. Provide the virus name, date of detection, and a description of how virus was detected:

_____

_____

5. Damage caused to your system, if any: _____

6. Damage or observations resulting when the virus triggers:_____

_____

7. List the anti-virus software and version used, to detect and identify the virus:

_____

   a. Method of clean up? _____

   b. Number of hours expended to remove the infection: _____

   c. Number and types of systems infected: _____

   d. How many floppies were found to be infected? _____

8. List LAN connections (PC/AppleTalk/Share/System 7), if any:_____

   a. Have file servers/nodes been checked for the infection? YES/NO/NA

9. Have all system users been notified of the infection? YES/NO/NA

10. Were system/user backup files checked for the infection? YES/NO

11. Suspected source of virus: _____

12. Final disposition: _____

13. Other locations, within or outside NRaD, possibly infected as a result of sharing infected magnetic media or files: _____

   a. Were these locations notified of possible infection? YES/NO/NA

14. Comments: _____

Forward completed form to DADPSSO and then on to Code 153 or userid "accredit".

Primary User: _____ Code _____ Extension _____

DADPSSO: _____ Code _____ Extension _____

FOR OFFICIAL USE ONLY (WHEN FILLED IN) 3/92

Page 1 of 1

Date ___/__/___

STRONGROOM/VAULT OPEN STORAGE CERTIFICATION QUESTIONNAIRE

This questionnaire is to be filled out prior to utilizing an area as a strongroom/vault for open storage of classified material. This questionnaire pertains to GENERAL SERVICE (GENSER) classified material only, all other requests must be submitted to Code 17. Approval may take 8- 12 weeks, depending on area modifications needed.

INFORMATION/INDUSTRIAL SECURITY:

1a. What level of GENSER classified material will be stored.

( ) TOP SECRET ( ) SECRET ( ) CONFIDENTIAL

1b. What special access categories stored?

( ) NONE
( ) LIMITED DISSEMINATION (LIMDIS)
( ) COMMUNICATIONS MATERIAL SYSTEMS (CMS)
( ) CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)
( ) NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN)
( ) WARNING NOTICE-INTELLIGENCE SOURCES INVOLVED (WNINTEL)
( ) NORTH ATLANTIC TREATY ORGANIZATION (NATO)
( ) FORMERLY RESTRICTED DATA (FRD)
( ) RESTRICTED DATA (RD)
( ) SINGLE INTEGRATED OPERATIONAL PLAN-EXTREMELY SENSITIVE INFORMATION (SIOP-ESI)

2. What is the building/room number of the area to be certified.

Building _____ Room _____ Site _____

3. Who are the individuals that will be responsible for the area?

Primary _____ Code _____ Phone _____

Alternate _____ Code _____ Phone _____

4. Will cleared contractors be working in the area without escort?

( ) YES ( ) NO

5. If answer to 4 is YES, provide following information. Attach additional sheet if necessary.

COMPANY NAME	CONTRACT NUMBER	SUBCONTRACTOR	(YES/NO)

6. Will any contractors identified above be afforded unescorted after hours access or require combination(s) to area?

( ) YES ( ) NO

7. Are all contractors on the same task?

( ) YES ( ) NO

8. Have procedures been developed to restrict access among personnel of different contract companies to company proprietary or contractually sensitive data? If so, explain procedures.

( ) YES ( ) NO ( ) N/A

9. Will all personnel (government and contractor) have a common need-to-know for all classified material? If not, how will the non-shared classified material be protected.

( ) YES ( ) NO

10. If answer to 9 is YES, who will certify, in writing, the universal need-to-know?

Name _____ Code _____ Phone _____

11. How will the custodian maintain individual accountability of classified material within this area?

AIS SECURITY:

1. Will classified data be processed on Automated Information Systems?

( ) YES ( ) NO
If NO, skip questions 2. - 9. of this section.

2. Will classified processed on Automated Information System be stored on hard drive?

( ) YES ( ) NO

3. Is AIS connected to any external networks/LANS/WANS? If YES, which ones? Provide network connectivity cable diagram.

( ) YES ( ) NO

4. Systems connected to networks/LANS/WANS must be disconnected. How will this requirement be met?

( ) N/A

_____

_____

5. Is AIS currently accredited? If YES, at what level? Provide SIN number(s). Attach additional sheet if more space needed.

( ) YES ( ) NO

SIN #	LEVEL I	LEVEL II	LEVEL III
_____	( )	( )	( )
_____	( )	( )	( )
_____	( )	( )	( )
_____	( )	( )	( )

6. TEMPEST requires 6 foot separation between system and telephones, data cables, t-box, modems, etc. Can this TEMPEST requirement be met? If not, why?

( ) YES ( ) NO

_____

_____

7. Does area have radios, floor heaters, any other small electrical devices?

( ) YES ( ) NO

8. Does system share peripheral devices (e.g., printers, plotters, etc.)?

( ) YES ( ) NO

9. If you haven't notified your DEPT/DIV ADP System Security Officer (DADPSSO) of this request, recommend you do so now.

PHYSICAL SECURITY:

1. Are the doors constructed of metal or solid wood?

( ) YES ( ) NO

2. Do doors to the area currently have Group 1/1R three position combination locks installed?

( ) YES ( ) NO

3. Are door louvers and baffle plates reinforced with wire mesh (No. 9 gauge, 2-inch-square mesh)?

( ) YES ( ) NO ( ) N/A

4. Are the walls made of plaster; gypsum board; metal; hardboard; wood; plywood; No. 9 gauge, 2-inch wire mesh or stronger; or other materials?

( ) YES ( ) NO

5. Does the area have insert type panels to separate areas?

( ) YES ( ) NO

6. Do window openings have bars and cross bars to prevent spreading or covered with No. 9 gauge mesh?

( ) YES ( ) NO

7. Are windows opaque?

( ) YES ( ) NO

8. Are there ducts, registers, sewers, or tunnels a size and shape that would permit unauthorized entry? Are any of the openings larger than 96 sq. inches?

( ) YES ( ) NO

9. Does the area currently have a security alarm system installed? If so, what is the line number and RTU number (alarm zone)?

( ) YES _____ ( ) NO

10. Attach a copy of the current security operations procedures including, floor plan for the area. The floor plan must include the locations of all doors, interior walls/partitions and windows.

Return completed form to Code 1504, Bldg. 33, Room 2223.

_____	_____	_____
REQUESTER	CODE	TELEPHONE #

==========

FOR CODE 15 USE ONLY.

Code 152 - approved/disapproved. _____ _____
SIGNATURE DATE

Reason:

_____

_____

Code 153 - approved/disapproved. _____ _____
SIGNATURE DATE

Reason:

_____

_____

Code 154 - approved/disapproved. _____ _____
SIGNATURE DATE

Reason:

_____

_____

Ser_____
Date_____

MEMORANDUM

From: Head, Department/Division Code _____
To: NRaD ADPSO, Code 0353

Subj: NETWORK SECURITY OFFICER APPOINTMENT

Ref: (a) NOSCINST 5500.1A, Chapter 13

1. In accordance with reference (a), the following NRaD employee is appointed Network Security Officer (NSO)/Assistant Network Security Officer (indicate assignment) for the Code _____ network, named: _____.

Name:_____
Building/Room:_____
Mail Code:_____
Extension:_____
Signature authority: YES or NO (for Assistant NSO only)
Name of NSO/Assistant NSO being replaced (if applicable):

_____

SIGNATURE

Copy to:
Outgoing NSO/Assistant NSO
Incoming NSO/Assistant

Ser_____
Date_____

MEMORANDUM

From: Head, Department/Division Code _____
To: NRaD ADPSO, Code 0353

Subj: DEPARTMENT/DIVISION ADP SYSTEM SECURITY OFFICER APPOINTMENT

Ref: (a) NOSCINST 5500.1A, Chapter 13

1. In accordance with reference (a), the following NRaD employee is appointed DADPSSO/Assistant DADPSSO (indicate assignment) for Code(s) _____.

Name:_____
User ID:_____
Building/Room:_____
Mail Code:_____
Extension:_____
Database access: YES or NO (for Assistant DADPSSO only)
Signature authority: YES or NO (for Assistant DADPSSO only)
Name of DADPSSO/Assistant DADPSSO being replaced (if applicable):

_____

SIGNATURE

Copy to:
Outgoing DADPSSO/Assistant DADPSSO
Incoming DADPSSO/Assistant DADPSSO

Page 1 of 1

MINIMUM SECURITY SAFEGUARDS FOR UNIX SYSTEM ADMINISTRATOR

- User and system files should be backed up on a regular scheduled basis. Extra copies of backups should be made and stored in a secure remote location for disaster recovery purposes.

- NO classified data should be stored on an "internal" hard disk, unless the computer is physically located in an area currently approved in writing for Secret Open Storage.

- Computers running any flavor of the UNIX Operating System must identify and authenticate users during login by requesting a USER- ID and PASSWORD. System audit logs (syslog) must be activated.

- The System Administrator must ensure that users select strong passwords that are a minimum of six characters and are not easy to guess. Recommend passwords be system random generated. Remind users to ensure correct file permissions are set on their classified files based on security clearance and need-to-know requirements. Recommend users files be created using a Umask value of 037 or 077.

- Magnetic media containing classified data, including working copies, must be labeled on the outside and internally to show the highest security classification contained on the media. A data description label will also be used. Media must show date created.

- Printouts, plots, and other hard copy must have the appropriate security classification marked/stamped at the top and bottom center of each page. Declassification instructions will be marked/stamped at the bottom of the first page. Hard copy must show date created.

- Classified working papers will be marked/stamped at the top and bottom center with appropriate security classification, working papers indicator and date created.

- Classified material must be locked in a secure container approved for storage of Secret material, when the work space is not occupied, unless the material is located in an area approved in writing for Secret Open storage.

- All unclassified and sensitive unclassified media and hard copy will be marked appropriately when used in a classified and unclassified processing environment.

- If the office space is cleaned by contractor personnel, an appropriately cleared NRaD employee must be present during cleaning.

- Recommend posting "Restricted Area - Authorized Personnel Only" sign . Ensure all entrants have proper clearance and need-to-know during classified processing.

- Ensure TEMPEST separation requirements are being maintained. Nearby electronic devices (e.g., radios, tape players, typewriters), must not be plugged in, telephones must be 3 feet from system, and when possible, system should not be sharing power outlets with other equipment.

- Prior to release or disposal of equipment (e.g., CPU, monitors, printers, plotters) or media (e.g., magnetic media, laser jet cartridges), ensure NRaD ADPSO approved declassification procedures have been followed and all labels removed.

- Ensure classified and sensitive unclassified hard copy documentation are disposed of following proper procedures. Prior to disposal, contact your DADPSSO or Code 0353.

- A warning banner must be posted (i.e., electronically on monitor at log-in time) to notify user about prohibitions when using system in an unauthorized way.

- Recommend all the "secure" keywords in the /etc/ttytab file be removed so that root login's are rejected. Super User access should be obtained using the "su" command, and all requests for "su" access to root must be recorded in a system audit log for review. In the /etc/group file or NIS map only the system administrator(s) should be listed as members of the wheel group (group 0).

- The most recent copy of the NOSC Security Policy and Plans Handbook (SPPH), must be kept near the computer. Refer to the handbook for security safeguards and procedures not covered by this enclosure.

- Run a password checking program such as "Crack" to check for user passwords that are easy to guess. Contact Code 914 for details.

- Make sure system "default" accounts have the default password changed (i.e. sys, bin).

- Disable or remove dormant user accounts no longer needed.

- Check the files /etc/hosts.equiv, /etc/hosts.lpd for a "+" sign and remove any that you find. No /.rhosts file should be created on a classified system.

- Regularly check the Syslog files for security violations or anomalies (i.e. repeated log in failures, bad SU attempts, Root log-in failures). Refer to /var/adm/messages or /usr/adm/messages.

- Before installing system software, thoroughly review software installation Script files for possible security problems (i.e. default passwords assigned, new privileged accounts created).

- Regular review of system password files to search for accounts or privileges that are not authorized. Also check for extra UID 0 accounts and accounts with a null (no) password.

- Ensure that all current system patches/fixes have been installed to correct previously reported security holes. Contact Code 0353 for information.

- Run the COPS security auditing program on the system on a regular basis to generate a report of existing security vulnerabilities. Correct all serious security problems listed on the output report.

- Ensure the file /etc/exports is writable only by Root.

- Check system documentation to establish the correct file and directory protections and ownership for system files and directories.

- Workstations must not be left logged in and unattended. Users must log off the workstations when their processing session is completed.

- Recommend assigning a LAN administrator to administer all workstations on the local network. Only the administrator and one alternate should be allowed to have "root" access to the user's workstations.

- Strongly recommend each workstation user and the LAN administrator review Chapters 2, 4, and 6 of the Sun Security Manual, Revision A of 9 May 1988.

- Suspected/actual security violations must be reported to your DADPSSO or the NRaD ADPSO, Code 153 as soon as possible.

- IF you are using SUN NFS:

- Be sure there is an * in the password field of any line beginning with a "+" symbol in both the password and group files on any NIS client.

- Be sure there is NO line beginning with a "+" in the password or group files on any NIS server.

- Use the Netgroups mechanism to restrict the export (and thus the ability to remotely mount) of file systems to a small set of local machines.

- To check a system for exports to the "world", run "showmount -e <host>". If the results show an export to (everyone), modify the /etc/exports file to provide the appropriate restrictions.

- Mount partitions "nosuid" unless SUID access is absolutely necessary.

- Never export a mounted partition on your system to an untrusted machine if it has any world- or group-writable directories.

- Do not use the root= option when exporting filesystems unless absolutely necessary.

- Use "fsirand" on all partitions that are exported.

- When possible, use the "secure" option for remote mounts.

MINIMUM SECURITY SAFEGUARDS FOR VMS SYSTEM MANAGERS

- The VMS Operating System must enforce Identification & Authentication by requiring a userid and password before a user can login. User passwords must be a minimum of eight (8) characters, preferably system random generated. Enabling/activation of system Audit logs, and a regular thorough review of these audit logs for security violations/anomalies by system management is required.

- The following Events must be audited as a minimum AUDIT, ACL, AUTHORIZATION, FILE_ACCESS=BYPASS, GRPPRV, READALL, FAILURE, LOCAL, BATCH, LOGINS, LOG FAILURES.

- Put ACE ACL access alarms on certain critical VMS System files for (write, delete, successful/unsuccessful) Some recommended VMS System files to be audited: [SYS$SYSTEM] SYS.EXE, LOGINOUT.EXE, STARTUP.COM, RIGHTSLIST.DAT [SYS$LIBARY] SECURESHR.EXE [SYS$ROOT] SYSEXE.DIR, SYSLIB.DIR, SYSMGR.DIR

- Set Audit alarms for all BREAKIN's. Enable Accounting to record all default activities to the Accounting Log for review.

- The SYSUAF, RIGHTSLIST, and other critical System files must be protected from unauthorized access.

- Security Alarm (OPCOM) messages should be routed to a security operator hard copy terminal. The terminal should be located in a secure area where it can be monitored regularly for suspicious or unusual activity.

- Strongly recommend you advise users to include the /ERASE qualifier when using the DELETE/PURGE commands to delete a classified file. Or turn on the feature to guarantee erase-on-delete by using the DCL command SET VOLUME/ERASE_ON_DELETE.

- The use of an ACL is required to share classified files with users not in the same Group, on a need-to-know basis. NO classified file should have World access.

- The security auditing program called "VMS Security Profile Inspector" should be run on the system on a regular basis. All identified security vulnerabilities must be corrected as soon as possible. Ensure that all current system patches/fixes have been installed to correct previously reported VMS security holes. (Contact Code 153 for info on where to obtain the VMS SPI software).

- User and system disk files should be backed up on a regular scheduled basis. Extra copies of backups should be made and stored in a secure remote location for disaster recovery purposes.

- Regular preventive maintenance should be performed on all ADP equip- ment, especially the disk drives to help prevent disk I/O errors.

- Users must be reminded not to leave a terminal logged in and unattended. The user should log off and clear the terminal screen when their processing session is completed.

- NO classified information may be stored on internal hard drives, unless the work space where the system is located is first approved in writing for Secret Open storage.

- Magnetic media containing classified data, including working copies, must be labeled on the outside and internally to show the highest classification contained on the media. A data description label will also be used. Media must show date created.

- Printouts, plots, and other hard copy must have the appropriate security classification marked/stamped at the top and bottom center of each page. Declassification instructions will be marked/stamped at the bottom of the first page. Hard copy must show date created.

- Classified working papers will be marked/stamped at the top and bottom center with appropriate security classification, working papers indicator and date created.

- Classified material must be locked in a secure GSA container approved for storage of Secret material, when the work space is not occupied, unless the material is located in an area approved in writing for open storage.

- If the facility is cleaned by contractor personnel, an appropriately cleared NRaD employee must be presenting during the cleaning.

- Recommend posting "Restricted Area- Authorized Personnel Only" sign. Ensure all entrants have proper clearance and need-to-know during classified processing.

- Ensure TEMPEST separation requirements are being maintained. Nearby electronic devices (e.g. radios, tape players, typewriters), must not be plugged in, telephones must be 3 feet from system, and when possible system should not be sharing power outlets with other equipment.

- A warning banner must be posted (i.e. electronically on monitor at login time) to notify user about prohibitions when using system in an unauthorized way.

- Prior to release or disposal of equipment (e.g. CPU, monitors, printers, plotters) or media (e.g. magnetic media, laser jet cartridges), ensure NRaD ADPSO approved declassification procedures have been followed and all labels removed.

- Ensure classified and sensitive unclassified hard copy documentation are disposed of following proper procedures. Prior to disposal, contact your DADPSSO or Code 153.

- The most recent copy of the NOSC Security Policy and Plans Handbook (SPPH), must be kept near the computer. Refer to this handbook for security safeguards and procedures not covered by this enclosure.

02/10/93

MINIMUM SECURITY SAFEGUARDS FOR SENSITIVE UNCLASSIFIED PROCESSING

- The user should back up their critical disk files on a regular scheduled basis. Extra copies of backups should be made and stored in a secure remote location for disaster recovery purposes.

- The user should obtain and use an effective Anti-Virus program which is available through computer Resource Center (CRC). The program should be used to scan all diskettes before booting, loading or executing software from the diskette.

- Offices spaces and other work areas with Sensitive Unclassified Processing will be locked when unattended and at the end of the workday.

- Computers with system keylocks installed should be locked when the area is unoccupied.

- All magnetic media containing Sensitive Unclassified data must have a label affixed to the outside, which indicates the appropriate sensitivity level of the data (e.g., For Official Use Only, Limited Distribution).

- Hardcopy containing Sensitive Unclassified data will have the appropriate sensitivity level marked/stamped at the bottom on the outside of the front cover (if any), on the first page, on the back page and on the outside of the cover (if any).

- Magnetic media containing Privacy Act data will have "Personal Data-Privacy Act of 1974" clearly labeled on the outside of the media.

- Printed output containing Personal data must have Privacy Act marking as shown above, on the top of each page.

- All Sensitive Unclassified material will be locked away in a secure container (e.g., locked desk, locked cabinet) when the work space area is unattended.

- All magnetic media containing sensitive unclassified data will be purged using NRaD ADPSO approved procedures and all identifying labels removed prior to disposal.

- All hardcopy documentation containing sensitive unclassified data can be disposed of by tearing, pulping, shredding or macerating to preclude recognition or reconstruction or, as a minimum disposed of by placing in a burn bag.

- The most recent copy of the NOSC Standard Security Policy and Plans Handbook (SPPH), must be kept near the computer. The user should consult the handbook for security safeguards and procedures not covered by this enclosure.

MINIMUM SECURITY SAFEGUARDS FOR CLASSIFIED PROCESSING

- Users should back up their critical files on a regular scheduled basis. Extra copies of backups should be made and stored in a secure remote location for disaster recovery purposes.

- Users should obtain and use an effective Anti-Virus program, which is available from either of the Computer Resource Centers (CRC). The program should be used to scan all diskettes before booting, loading or executing software from the diskette.

- Prior to processing classified data, the T-box data cable or ethernet cable must be disconnected from the back of the computer. Place the T-Box, data cable and power cable at least 3 feet from the computer and its peripherals. The T-Box power cable should be plugged into a separate power outlet other than the one used by the computer and its peripherals.

- Classified data will not be stored on an internal hard drive. If a classified file should be inadvertently written to the hard disk, the user should immediately contact their DADPSSO for assistance in declassifying the hard drive.

- Recommend using a copy of the PROTECT.COM (PCs) or LOCKDISK CDEV (MACs) software program to help reduce the chances of a classified file being written to the internal hard drive during classified processing. These software programs are available from the NRaD BBS or CRC.

- Magnetic media containing classified data, including working copies, must be labeled on the outside and internally to show the highest security classification contained on the media. A data description label will also be used. Media must show date created.

- Printouts, plots, and other hard copy must have the appropriate security classification marked/stamped at the top and bottom center of each page. Declassification instructions will be marked/stamped at the bottom of the first page. Hard copy must show date created.

- Classified working papers will be marked/stamped at the top and bottom center with appropriate security classification, working papers indicator and date created.
- Classified material must be locked in a GSA approved container when the work space is not occupied, and at the end of the work day, unless the material is located in an area approved in writing for open storage.

- Classified magnetic media and hard copy over 90 days old will be bar coded and controlled through the document control system or will be destroyed following proper procedures.

- All unclassified and sensitive unclassified media and hard copy will be marked appropriately when used in a classified and unclassified processing environment.

- Work spaces will be locked when unattended and at the end of the work day. Computers that have a system key lock installed should be locked when the work area is not occupied.

- If the office space is cleaned by contractor personnel, an appropriately cleared NRaD employee must be present during cleaning.

- Recommend posting "Restricted Area - Authorized Personnel Only" sign. Ensure all entrants have proper clearance and need-to-know during classified processing.

- Maintain system audit log (manual, automated, or combination) of system activity during classified or sensitive unclassified processing.

- Recommend maintaining operating system and applications software on removable media (e.g., Bernoulli, SYQUEST) and use for booting when processing classified data.

- Applications software (e.g., word processing, spreadsheet, graphics) must have automatic backup default set to other than the internal hard disk drive. Contact either of the CRC's for assistance.

- Ensure TEMPEST separation requirements are being maintained. Nearly electronic devices (e.g., radios, tape players, typewriters), must not be plugged in, telephones must be 3 feet from the system, and when possible, system should not be sharing power outlets with other equipment.

- Any unclassified computer that is sharing peripheral devices with a classified system via an A/B switch box, must be physically disconnected from the switch box. Also, physically disconnect any internal/external modem from the computer prior to processing classified data.

- Prior to processing classified data, ensure the computer is physically disconnected from any unclassified network.

- After classified processing ensure the computer and peripheral devices are powered down to purge resident classified data. Remove printer ribbons and protect as classified, and run 3-full pages of continuous text through laser jet printers after classified use.

- Prior to release or disposal of equipment (e.g., CPU, monitors, printers, plotters) or media (e.g., magnetic media, laser jet cartridges), ensure NRaD ADPSO approved declassification procedures have been followed and all labels removed.

- Ensure classified and sensitive unclassified hard copy documentation are disposed of following proper procedures. Prior to disposal, contact your DADPSSO or Code 153.

- System(s) shared by multiple users should have an "Authorized Access List" posted near system(s).

- A warning banner must be posted (i.e., physically at system or electronically on monitor at log-in time) to notify user about prohibitions when using system in an unauthorized way.

- The most recent copy of the NOSC Standard Security Policy and Procedures Handbook (SPPH) must be kept near the computer. Consult the handbook or contact your Department/Division ADP Security officer (DADPSSO) for further guidance or questions.

Date __/__/__

MEMORANDUM

From: Code _____ DADPSSO
To: Code 0353

Subj: SECURE FACSIMILE AND STU-III QUESTIONNAIRE

1. Prior to transmitting or receiving classified data electronically, written approval must be obtained from Code 0353. The following information shall be provided for all secure facsimile attached to a STU-III, or a FAX/STU-III attached to an accredited AIS.

a. Facsimile information:
Manufacturer: _____
Model: _____
Bar Code: _____
Serial Number: _____
Building: _____ Room: _____ Site: _____
Primary User: _____ Code: _____
Custodian: _____ Code: _____

b. STU-III or STU-III Data Device information:
Manufacturer: _____
Model: _____
Serial Number: _____
SACS activated: YES/NO
Building: _____ Room: _____ Site: ____
Primary User: _____ Code: _____
Custodian: _____ Code: _____

c. AIS information:
SIN: _____ Bar Code: _____

d. Type of data (check all that apply):
( ) TOP SECRET
( ) SECRET
( ) CONFIDENTIAL

Special Access Category
( ) NATO ( ) NOFORN
( ) WNINTEL ( ) OTHER _____

e. Comments. _____

_____

3/93

Page 1 of 1

SECURITY OPERATING PROCEDURES
SECURE FACSIMILE (FAX) TO SECURE TELEPHONE UNIT (STU)-III

1. FAX/STU-III's will not be moved or reconfigured until approval is received from STU-III Manager Code 03532, and Code 0353.

2. The FAX and STU-III are to be operated primarily during regular work hours although operation at other hours may be necessary. The FAX and STU-III will not be operated in an unattended mode unless a STU-III access control system (SACS) is being used in the enabled mode. The SACS feature will not be authorized unless the system is located in an area certified for open storage of classified material.

3. If the FAX machine does not contain memory storage other than preset functions. Clearing of memory storage at the end of the day or when the room is not attended is not required.

4. In the absence of a SACS, protection of the Crypto Ignition Key (CIK) when inserted in the STU-III shall be ensured by continuous attendance. When the area is unoccupied, the CIK shall be in the possession of the authorized user or locked in an approved storage container.

5. The STU-III Manager will be contacted when maintenance or repair of the STU-III is required. Proper area sanitizing will be implemented during times of any maintenance activity.

6. Suspected insecurities will be reported to the STU-III Manager Code 03532, ext. 34740, during normal working hours, or via CDO, x34621 after normal working hours.

7. Provisions shall be implemented to ensure system/data integrity is maintained during system usage. Before transmission of classified information takes place, the user must be certain the party at the distant end STU-III has the appropriate security clearance and need-to-know for the classified material to be transmitted. If a SACS unit is used with the SACS feature and the auto-answer more is activated, the system will verify the security level.

8. FAX/STU-III users shall provide access control for their data and enforce security requirements for their system. Physical security and access control to the area where classified operations take place shall be maintained during FAX operations.

9. The FAX machine must have passed a TEMPEST visual.

10. Appropriate marking and documentation of classified material being sent and received is required. All outgoing material shall be marked with the security classification; date created; the classification authority; the downgrading/declassification indicator; and the paragraph, page, and portion markings.

11. A record of all incoming and outgoing classified transmissions must be maintained for each FAX/STU-III system and must contain the following information:

a. Date and time received or transmitted.
b. Sent to/sent from (name, activity, phone number, and code).
c. Classification of material.
d. Unclassified subject of title of material.
e. Person sending material.
f. For outgoing Secret material already controlled, the S-numbers and, when assigned, bar codes.

12. A copy of the facsimile transmission sheet or machine generated transmission report will satisfy the requirement of item 11, as long as it contains or is annotated to include all of the above information. However, incoming Secret facsimiles retained in excess of 90 days must be immediately barcoded and entered into the NRaD classified document control system. The record of incoming and outgoing classified transmissions must be maintained for 6 months from date of transmission.

13. Any outgoing or incoming transmission of Top Secret material must be coordinated, in advance, with the Top Secret Control Officer (TSCO). If Top Secret material is received without this advance Coordination, immediately notify the TSCO so that appropriate accountability and storage of the material is accomplished.

14. Only a verbal acknowledgment of receipt for the transmitted classified document(s) is required from the person receiving the document at the distant end. If a STU-III unit is used with the SACS feature enabled, acknowledgment is not required.

15. All incoming transmissions received without a security classification, will be handled and safeguarded at the highest classification level authorized for the STU-III when the CIK is inserted. Verification of the actual classification of transmitted documents received, must be obtained from the originator of the document, as soon as possible.

16. FAX system users shall ensure the proper storage of classified material or media when the room is not occupied.

17. When a FAX/STU-III are operating at a classified level, only properly cleared personnel with authorization and need-to-know may access the system area. A posted authorized access list must be maintained near the system area.

9/92

SECURITY OPERATING PROCEDURES
AUTOMATED INFORMATION SYSTEMS (AIS) TO
SECURE TELEPHONE UNIT (STU)-III

1. AIS/STU-III's will not be moved or reconfigured until approval is received from STU-III Manager Code 03532, and Code 0353.

2. The AIS and STU-III are to be operated primarily during regular work hours although operation at other hours may be necessary. The AIS and STU-III will not be operated in an unattended mode unless a STU-III access control system (SACS) is being used in the enable mode. The SACS feature will not be authorized unless the system is located in an area certified, in writing, for open storage of classified material.

3. In the absence of a SACS, protection of the Crypto Ignition Key (CIK) when inserted in the STU-III shall be ensured by continuos attendance. When the area is unoccupied, the CIK shall be in the possession of the authorized user or locked in an approved storage container.

4. The STU-III Manager will be contacted when maintenance or repair of the STU-III is required. Proper area sanitizing will be implemented during times of any maintenance activity.

5. Suspected insecurities will immediately be reported to the STU-III Manager Code 03532, ext. 34740, during normal working hours, or via CDO, x34621, after normal working hours.

6. Provisions shall be implemented to ensure system/data integrity is maintained during system usage. Before transmission of classified information takes place, the user must be certain the party at the distant end STU-III has the appropriate security clearance and need-to-know for the classified material to be transmitted. If a SACS unit is used with the SACS feature and the auto-answer mode is activated, the system will verify the security level.

7. AIS and STU-III users shall provide access control for their data and enforce security requirements for their system. Physical security and access control to the area where classified operations take place shall be maintained during classified operations.

8. The computer system must have passed a TEMPEST visual and have prior written approval from the Designated Approval Authority (DAA) to process classified data.

9. The cable connecting a computer to a STU-III data port must be shielded in accordance with NACSIM 5203.

10. Verify that the remote AIS being accessed, and the local NRaD AIS are authorized to process data at the same maximum security level (i.e., a computer approved to process SECRET data may not be connected to a computer authorized to process TOP SECRET). System user must receive written verification of remote system approval prior to transmission or receipt of classified data.

11. While connected to a remote computer, the local and remote system users will ensure communications program (i.e., Kermit, ProComm) are not operating in the server or host mode of operation.

12. Classified material being sent and received, must be appropriately marked and documented. All outgoing material shall be marked with the security classification; date created; the classification authority; the downgrading/declassification indicator; and the paragraph, page, and portion markings.

13. A record of all incoming and outgoing classified transmissions must be maintained for each AIS/STU-III system and must contain the following information:

a. Date and time received or transmitted.
b. Sent to/from (name, activity, phone number, and code).
c. Classification of material.
d. Unclassified subject or title of material.
e. Person sending material.
f. For outgoing Secret material already controlled (in hard copy form), the S-numbers and, when assigned bar codes.

14. The record of incoming and outgoing classified transmissions must be maintained for 6 months from date of transmission.

15. After transmitting a classified document(s) to the distant end, only a verbal acknowledgment of receipt is required from the person receiving the document. If a STU-III unit is used with the SACS feature enabled, acknowledgment is not required.

16. All incoming transmissions received without a security classification, will be handled and safeguarded at the highest classification level authorized for the STU-III when the CIK is inserted. Verification to determine the actual classification must be obtained form the originator of the file, as soon as possible.

17. All incoming SECRET transmissions printed for hardcopy retention beyond 90 days, will be immediately barcoded and entered into the NRaD classified document control system.

18. All incoming classified transmissions will be stored on removable magnetic media unless the system is approved, in writing, to operate in an area certified for open storage of classified material.

19. All magnetic media containing classified data in excess of 90 days, will be barcoded and entered into NRaD classified document control system.

20. AIS system user shall ensure the proper storage of classified material or media when the room is not occupied.

21. When an AIS/STU-III are operating at classified level, only properly cleared personnel with authorization and need-to-know may access the system area. A posted authorized access list must be maintained in the system area.

22. A copy of the most recent NOSC Standard Security Policy and Plans Handbook (SPPH) must be in the area of the computer.

4/92

SECURITY TEST & EVALUATION (ST&E) PLAN
AIS PROCESSING SENSITIVE UNCLASSIFIED DATA

CODE _____ SIN_____ BAR CODE NUMBER _____
BUILDING _____ ROOM/LAB _____ SITE _____

AIS SECURITY COUNTERMEASURES	YES	NO	N/A
ACCESS			
1. A current list of system users is posted.	[ ]	[ ]	[ ]
2. System access warning message is displayed.	[ ]	[ ]	[ ]
3. An audit log is maintained.	[ ]	[ ]	[ ]
4. Audit log is reviewed regularly.	[ ]	[ ]	[ ]
5. Access is controlled by user ID/password(s).	[ ]	[ ]	[ ]
6. Password(s) are not posted on or near system.	[ ]	[ ]	[ ]
ENVIRONMENTAL			
1. Fire protection equipment is within 50 feet.	[ ]	[ ]	[ ]
2. Firm alarm lever/switch is located nearby.	[ ]	[ ]	[ ]
3. System area is kept clean of dust/dirt.	[ ]	[ ]	[ ]
4. Protective system covers are available.	[ ]	[ ]	[ ]
5. Equipment is operated within temperature range.	[ ]	[ ]	[ ]
DATA/MEDIA (PRINTED/MAGNETIC)			
1. Data/Media is properly marked.	[ ]	[ ]	[ ]
2. Data is stored on removable media.	[ ]	[ ]	[ ]
3. Data/Media is stored in locked container.	[ ]	[ ]	[ ]
4. AIS protected by system/disk key lock.	[ ]	[ ]	[ ]
5. System warning labels are displayed.	[ ]	[ ]	[ ]
6. User knows of media clearing procedures.	[ ]	[ ]	[ ]
7. User knows of proper disposal procedures.	[ ]	[ ]	[ ]
8. Operating system/files are backed up regularly.	[ ]	[ ]	[ ]
PHYSICAL			
1. System is turned off when unattended.	[ ]	[ ]	[ ]
2. Area is secured when unattended.	[ ]	[ ]	[ ]
AWARENESS			
1. SPPH or SOP available in system area.	[ ]	[ ]	[ ]
2. All software tested for virus infection.	[ ]	[ ]	[ ]
3. User abides by copyright/license agreements.	[ ]	[ ]	[ ]
4. User receives regular security training.	[ ]	[ ]	[ ]
5. User knows to report problems to their DADPSSO.	[ ]	[ ]	[ ]

Comments _____

_____

Based upon the above test results, the overall rating is:

PASS/FAIL

FOR OFFICIAL USE ONLY - WHEN FILLED IN 3/93

Page 1 of 1

SECURITY TEST & EVALUATION (ST&E) PLAN
MICROCOMPUTERS PROCESSING CLASSIFIED DATA

CODE ____ SIN _____ BAR CODE NUMBER _____
BUILDING ____ ROOM/LAB _____ SITE _____

AIS SECURITY COUNTERMEASURES	YES	NO	N/A
ACCESS			
1. A current list of system users is posted.	[ ]	[ ]	[ ]
2. List is updated regularly.	[ ]	[ ]	[ ]
3. System warning banner is displayed prior to login.	[ ]	[ ]	[ ]
4. Access is controlled by user ID/password(s).	[ ]	[ ]	[ ]
5. PROTECT.COM/LOCKDISK CDEV write protection software is used.	[ ]	[ ]	[ ]
6. Operating system is booted from removable media.	[ ]	[ ]	[ ]
7. Files are backed up regularly.	[ ]	[ ]	[ ]
8. User clears RAM after classified processing.	[ ]	[ ]	[ ]
ENVIRONMENTAL			
1. Fire protection equipment is within 50 feet of area.	[ ]	[ ]	[ ]
2. Fire alarm lever/switch is located nearby.	[ ]	[ ]	[ ]
3. AIS is connected to power surge protector.	[ ]	[ ]	[ ]
DATA/MEDIA (PRINTED/MAGNETIC)			
1. All data/media are properly marked.	[ ]	[ ]	[ ]
2. Data is stored on removable media.	[ ]	[ ]	[ ]
3. Data/Media are stored in a GSA approved container.	[ ]	[ ]	[ ]
4. Data/Media over 90 days old are properly controlled.	[ ]	[ ]	[ ]
5. User knows of media declassification procedures.	[ ]	[ ]	[ ]
6. User knows of proper disposal procedures.	[ ]	[ ]	[ ]
PHYSICAL			
1. Area is certified in writing for Open Storage.	[ ]	[ ]	[ ]
2. Area access restricted based on need-to-know.	[ ]	[ ]	[ ]
3. Monitors are protected from non/casual access.	[ ]	[ ]	[ ]
4. Doors are closed during classified session.	[ ]	[ ]	[ ]
5. Blinds or window coverings are closed during session.	[ ]	[ ]	[ ]
6. Visitors are escorted when required.	[ ]	[ ]	[ ]
VIRUS			
1. Virus detection software is available and used.	[ ]	[ ]	[ ]
2. User knows to report virus infection to DADPSSO.	[ ]	[ ]	[ ]
EMANATIONS			
1. Classified cables are separated from unclassified cable by no less than one meter (3 feet).	[ ]	[ ]	[ ]
2. Disconnected equipment or cables are moved no less than 1 meter from AIS.	[ ]	[ ]	[ ]
3. AIS is powered by dedicated power source.	[ ]	[ ]	[ ]
4. AIS does not share unclassified peripheral while processing classified data.	[ ]	[ ]	[ ]

AIS SECURITY COUNTERMEASURES	YES	NO	N/A
COMMUNICATIONS			
1. Network Security Officer is known.	[ ]	[ ]	[ ]
2. Network Security Officer has approved connection to classified network.	[ ]	[ ]	[ ]
3. Network Security Officer has provided SOP.	[ ]	[ ]	[ ]
4. Data encryption is done with NSA approved equipment.	[ ]	[ ]	[ ]
5. Users knows to control, properly mark and store all classified data received by STU-III or FAX.	[ ]	[ ]	[ ]
6. AIS disconnected from unclassified networks, modems or LANS prior to classified session.	[ ]	[ ]	[ ]
AWARENESS			
1. User knows who their DADPSSO is.	[ ]	[ ]	[ ]
2. SPPH or SOP are available in system area.	[ ]	[ ]	[ ]
3. User abides by copyright/license agreements.	[ ]	[ ]	[ ]
4. User receives regular security training.	[ ]	[ ]	[ ]
5. User knows to report problems to their DADPSSO or Code 0353.	[ ]	[ ]	[ ]

Comments/Deficiencies _____

_____

_____

_____

_____

_____

Based upon the above test results, the overall rating is:
PASS/FAIL

FOR OFFICIAL USE ONLY - WHEN FILLED IN

NRaD Information Systems Authorization Form

Return to the Computer Resource Center
(Instructions on Reverse Side)

Rev 6/93

Section 1 — User Information

First Name (Please Print or Type)	Middle	Last Name

Code	Phone	Bldg/Room

Job Order Number	Account

I request an account on: (Check all that apply)

Cod	
Humu	
Manta	
Marlin	
Wahoo	
Other	

Draco (Applications)

Requested Userid								

	Yes	No
PMSS General		
Contractor		

	Yes	No
TAC Access		

Company Name (If not NRaD employee):

Company Street Address, City, State, Zip Code:

NRaD Affiliation (Please X Only One):

Employee		Sponsor		Other Government		Military		Contractor	

Section 2 — NRaD Approving Authority

Signature (Branch Head or Above)	Print or Type Approving Name	Code	Phone	Date

Section 3 — User Security Statement

I agree to limit access to myfiles to project associates, who must also be registered system users. I understand that disclosure of my password to anyone else is a **SECURITY VIOLATION**. I will abide by **NOSCINST 5500.1A Chapter 13,** which can be obtained from your Branch or Division secretary.

User's Signature	Date

Section 4 — CRC Consultant Use Only

Assigned Userid	Programmer Number	Consultant	Date

NCAC Computer Account Request Form

Return to the NCAC Consultants Office Bayside Room B206, Bldg 1.

(Instructions on Reverse Side) Rev 6/93

Section 1 NCAC User Information

First Name (Please Print or Type)	Middle Init	Last Name

Code	Phone	Bldg/Room

Job Order Number	Account

I request an account on: (Check all that apply)

CLASSIFIED:

Cheetah	
Cougar (SGI)	
Jaguar (SGI)	
Leopard (SGI)	
Lynx (SGI)	
Other	

UNCLASSIFIED:

Stingray	
Ocelot (SGI)	
Panther (SGI)	
Puma (SGI)	
Other	

IS Userid								

	I do not have a IS account. (In addition to this form, you must complete the **IS Authorization Form.**)

Please describe why you need access to the NCAC resources (include Project Name.)

Section 2 NOSC Approving Authority

NCCOSC Approval Signature (Branch Head or Above)	Code	Date

Section 3 User Security Statement

I have read and understand the: (Check all that apply)

	Classified NCAC Security Policy and Procedures Handbook.
	Unclassified NCAC Security Policy and Procedures Handbook.

Signature	Date

Section 4 NCAC Consultant Use Only

Userid	Programmer Number	Consultant	Date

FACILITY CHANGE REQUEST (FCR)

FCR #

Originator: _____ Code/Phone # _____

Point of Contact: _____ Code/Phone # _____

Origination Date: / / (mm dd yy)

FCR Title: _____

Labs Affected: _____

Location (Floor grid reference or area): _____

Payment Responsibility: _____

Description (of what is required and options):

_____

_____

_____

_____

_____

_____

Justification/Purpose (include impact if "Disapproved"):

_____

_____

_____

Attachments:

_____

_____

Estimated Equipment/Software Delivery Date: _____

Required Completion Date: _____

Project Managers/Task Leaders Initial: _____

Considerations:

a. Space impact (change to laboratory floor plan), if yes, provide marked-up drawing.

b. Interface requirements: _____

Network connections: _____

HSDS changes: _____

c. Software version requirements: _____

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED

b. LEVEL OF SAFEGUARDING REQUIRED

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	Due Date (YYMMDD)

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

	a. ORIGINAL *(Complete date in all cases)*		Date (YYMMDD)
	b. REVISED *(Supersedes all previous specs)*	Revision No.	Date (YYMMDD)
	c. FINAL *(Complete Item 5 in all cases)*		Date (YYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [ ] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [ ] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		
b. RESTRICTED DATA		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		
d. FORMERLY RESTRICTED DATA		
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)		
(2) Non-SCI		
f. SPECIAL ACCESS INFORMATION		
g. NATO INFORMATION		
h. FOREIGN GOVERNMENT INFORMATION		
i. LIMITED DISSEMINATION INFORMATION		
j. FOR OFFICIAL USE ONLY INFORMATION		
k. OTHER *(Specify)*		
STUB NUMBER:		

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

DD Form 254, DEC 90 *Previous editions are obsolete.* 805/340

NRaD (O/P) 5500/3 (4-93)

STUB NUMBER: CONTRACT NUMBER: N66001- - -

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

[ ] Direct [XX] Through (Specify)

COMMANDING OFFICER, NCCOSC RDTE DIV 003, 53560 HULL ST, SAN DIEGO, CA 92152-5001

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review
* In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

COPIES OF ALL SUBCONTRACT DD FORM 254'S MUST BE PROVIDED TO THE DISTRIBUTION LISTED IN BLOCK 17.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) [XX] Yes [ ] No

SPECIFIC ON-SITE SECURITY REQUIREMENTS ARE ATTACHED.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) [ ] Yes [ ] No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
P. A. TALLEY	CONTRACTING OFFICER FOR SECURITY MATTERS	(619) 553-3195

d. ADDRESS (Include Zip Code)	e. SIGNATURE
COMMANDING OFFICER NCCOSC RDTE DIV 0352 53560 HULL ST SAN DIEGO CA 92152-5001	

17. REQUIRED DISTRIBUTION

XX	a. CONTRACTOR
	b. SUBCONTRACTOR
XX	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	d. U.S ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
XX	e. ADMINISTRATIVE CONTRACTING OFFICER NRaD CODE
XX	f. OTHERS AS NECESSARY NRaD CODES 0352,

DD Form 254 Reverse, DEC 90
NRaD (O/P) 5500/3 (4-93) (BACK)

*U.S GPO: 1991-848-013/40526

APPENDIX E

DEFINITIONS & ABBREVIATIONS

A

ACCESS—The ability and opportunity to obtain knowledge or possession of classified information. An individual does not have access to classified information merely by being in a place where such information is kept; provided that the security measures which are in effect prevents an individual who doesn't have a need to know from gaining possession of this classified information.

ACCREDITATION—A policy decision by the responsible designated approving authority (DAA) in a formal declaration that appropriate security countermeasures have been properly implemented for an automated information system (AIS) activity or network, so that the activity or network is operating at an acceptable level of risk.

ACTIVE DEVICE—In current loop applications, a device capable of supplying the current for the loop.

ADDRESS—A unique sequence of bits, a character, or a group of characters that identifies a network station, user, or application; a unique designation for the location of data; used mainly for routing purposes.

ADP—Automated Data Processing

ADPSO—Automated Data Processing Security Officer

ADP SECURITY—The measures required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of data (classified, personal, sensitive business), and loss of the ability to process data.

AIS—Automated Information System. An assembly of computer hardware, software or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data and information.

ANALOG—In communications, transmission employing variable and continuous waveforms to represent information values, where interpretation by the receiver is an approximation (quantification) of the encoded value; compare with digital.

ANSI (American National Standards Institute)—The principal standards development organization in the U.S.A; the U.S.A.'s member body to the ISO, ANSI is a nonprofit, independent body that is supported by trade organizations, professional societies, and industry; ANSI defined ASCII.

API (Application Program Interface)—A set of formalized software calls and routines that can be referenced by an application program to access underlying network services.

Apollo DOMAIN—A proprietary network operating system created by Apollo Computers (now Hewlett-Packard) and implemented as a 10 Mbps Token-Ring network over coax between Apollo workstations.

APPC (Advanced Peer-to-Peer Communications)— Uses Logical Unit (LU) 6.2; a network node definition by IBM®, featuring high-level program interaction capabilities on a peer-to-peer basis.

AppleTalk®—A proprietary computer networking standard promulgated by Apple® Computer for use in connecting Macintosh® computers and other peripherals, particularly LaserWriter® printers; operates at 230 kilobytes per second (Kbps) over phone wire or 10 megabytes per second (Mbps) over ethernet.

APPLICATION LAYER—The highest of the seven layers of the OSI model structure; contains all user or application programs; in the IBM® SNA, the end-user layer.

APPLICATION SOFTWARE—Programs that process or manipulate data; includes database managers, word processors, text editors, spreadsheets, and other programs that enable the useful production of data.

ARP (Address Resolution Protocol)— A Transmission Control Protocol Internet Protocol (TCP/IP) process that maps IP addresses to Ethernet addresses; required by TCP/IP for use with Ethernet.

ARPA (Advanced Research Projects Agency)—(formerly Defense Advanced Research Projects Agency) Developed the first major packet-switched network; operates within the U.S. Department of Defense.

ARQ (Automatic Request for Retransmission)—A communications feature whereby the receiver asks the transmitter to resend a block or frame, generally because of errors detected by the receiver.

ASCII (American Standard Code for Information Interchange)—A system used to represent alphanumeric data; a 7-bit-plus-parity character set established by ANSI and used for data communications and data processing; ASCII allows compatibility among data services; one of two such codes (see EBCDIC) used in data interchange. ASCII is normally used for asynchronous transmission.

ASYNCHRONOUS—Data transmission that is not related to the timing, or a specific frequency, of a transmission facility; transmission characterized by individual characters, or bytes, encapsulated with start and stop bits, from which a receiver derives the necessary timing for sampling bits; also, start/stop transmission.

ATM (Asynchronous Transfer Mode)—Proposed cell-relay telecommunications service where fixed-length 56 bit data packets are optimized for transmission though a wide are network. Initial data rate will be at 125 Mbps, but will grow to 600 Mbps and 1.2 Gbps.

ATTENUATION—The deterioration of signal strength, measured in decibels; opposite of gain.

B

BACKBONE NETWORK—A transmission facility designed to interconnect low-speed distribution channels or clusters of dispersed user devices.

BALUN (BALanced/UNbalanced)—In the IBM® cabling system, refers to an impedance-matching device used to connect balanced twisted-pair cabling with unbalanced coaxial cables.

BANDWIDTH—The difference, expressed in hertz (Hz), between the highest and lowest frequencies of a transmission channel.

Banyan-VINES®—A proprietary network operating system promulgated by Banyan Systems Inc., used to connect PC computers over LANs and WAN's. Primarily known for their StreetTalk® global naming directory service. This global naming service makes Banyan VINES particularly useful in building large networks. Because of this, it has been selected as a primary network operating system for the U S. Marine Corp's.

BASEBAND—A signal frequency below the point when the signal is modulated as an analog carrier frequency; in modulation, the frequency band occupied by the aggregate of the transmitted signals when first used to modulate the carrier (IBM®).

BATCH PROCESSING—A data-processing technique in which data is accumulated and processed in batches; contrast with interactive processing.

BIT (Binary Digit)—The smallest unit of information in a binary system; a bit can have a zero or a one value.

BIT DURATION—The time it takes one encoded bit to pass a point on the transmission medium; in serial communications, a relative unit of time measurement, used for comparison of delay times (e.g., propagation delay, access latency) where the data rate of a (typically high-speed) transmission channel can vary.

BPS (Bits per Second)—The basic unit of measure for serial data-transmission capacity, Kbps for kilo (thousands of) bits per second; Mbps for mega (millions of) bits per second; Gbps for giga (billions of) bits per second; Tbps for tera (trillions of) bits per second.

BREACH—A successful and repeatable defeat of security controls without discovery, which, if carried to consummation could result in a penetration of the system.

BRIDGE—A device that connects different local area networks at the data-link layer.

BROADBAND—Describing transmission equipment and media that can support a wide range of electromagnetic frequencies; typically, the technology of CATV transmission, as applied to data communications, that employs coaxial cable as the transmission medium and radio-frequency carrier signals in the 50- to 500-MHz range; any communications channel with a bandwidth greater than that of a voice-grade telecommunications channel; sometimes used synonymously with wideband.

BROADCAST—A method of transmitting messages to two or more stations at the same time, such as over a bus-type local area network or by satellite; protocol mechanism whereby group and universal addressing is supported.

BUFFERING—The process of temporarily storing data in a software program or in RAM, to allow transmission devices to accommodate differences in data transmission rates.

BUS—A transmission path or channel; an electrical connection, with one or more conductors, by which all attached devices receive all transmissions at the same time; a linear local area network topology, such as is used in Ethernet and the token bus, where all network nodes "listen" to all transmissions, selecting certain ones based on address identification.

BYTE—A unit of information, used mainly in referring to parallel data transfer, semiconductor capacity, and data storage; also referred to as a "character"; a group of eight (sometimes seven) bits used to represent a character.

C

C3—Command, Control and Communication

CATV —Community Antenna Television (CATV). Both broadband LANs and CATV systems use the same type of components: trunk and distribution cables, amplifiers, splitters, translators, etc. However, broadband networks typically extend over a limited area (building or campus), while a CATV system will extend over a wide area (often city-wide), and are franchised operations.

CCITT (Consultative Committee for International Telephony and Telegraphy)— An international association that sets worldwide communications standards (e.g., V.21, V.22, X.25, etc.).

CCTV—Closed circuit television (CCTV). Often surveillance cameras put on a CATV system or point-to-point cabling.

CHARACTER—A standard 8-bit unit representing a symbol, letter, number, or punctuation mark; generally means the same as byte.

CHARACTER-ORIENTED—Describing a communications protocol or a transmission procedure that carries control information encoded in fields of one or more bytes.

CHARACTERISTIC IMPEDANCE—The impedance termination of an (approximately) electrically uniform transmission line that minimizes reflections from the end of the line.

CHECKSUM—The total of a group of data items or a segment of data that is used for error-checking purposes. Both numeric and alphabetic fields can be used in calculating a checksum, since the binary content of the data can be added. Just as a check digit tests the accuracy of a single number, a checksum serves to test an entire set of data which has been transmitted or stored. Checksums can detect single-bit errors and some multiple-bit errors.

CLOCK—An oscillator-generated signal that provides a timing reference for a transmission link; used to control the timing of functions such as sampling interval, signaling rate, and duration of signal elements; an "enclosed" digital network typically has only one master clock.

CM—Configuration Management

CMS—Communications Security Materials System

COAXIAL CABLE—A popular transmission medium usually consisting of one central wire conductor (two, for twinaxial cable) surrounded by a dielectric insulator and encased in either a wire mesh or an extruded metal sheathing; coaxial cable comes in many varieties, depending on the degree of EMI shielding afforded and voltages and frequencies accommodated; common Community Antenna Television (CATV) transmission cable, typically supporting RF frequencies from 50 to about 500 MHz; also called "coax."

COMMUNICATIONS SERVER—An intelligent device (a computer) providing communications functions; an intelligent, specially configured node on a local area network designed to enable remote-communications access and exit for LAN users.

COMPRESSION—Any of several techniques that reduce the number of bits required to represent information in data transmission or storage (thus conserving bandwidth or memory), in which the original form of the information can be reconstructed; also called "compaction."

COMPROMISE—The known or suspected exposure of classified information or material to an unauthorized person.

COMPUTER SYSTEMS SECURITY—Includes all hardware / software functions, characteristic features, operational procedures, accountability procedures, access controls at the computer facility, management constraints, physical structures, devices, and personnel and communications controls needed to provide an acceptable level of protection for classified material to be contained in the system.

COMSEC—Communications Security

CONCENTRATOR—Any communications device that allows a shared transmission medium to accommodate more data sources than there are channels currently available within the transmission medium.

CONDITIONING—Extra-cost options that users may apply to leased, or dedicated, voice-grade telephone lines in which line impedances are carefully balanced; will generally allow for higher-quality or higher speed data transmission; in increasing order of resultant line quality and cost, conditioning may be C1, C2, C4, or D1; allows improved line performance with regard to frequency response and delay distortion.

CONFIGURATION MANAGEMENT—Refers to the process of documenting and maintaining control of the components of a system (hardware, software versions, setup parameters, connections, etc.).

CONTENTION—In communications, the situation when multiple users vie for access to a transmission channel, whether a PBX circuit, a computer port, or a time slot, within a multiplexed digital facility.

CORE—The central region of an optical wave guide through which light is transmitted; typically 8 to 12 microns in diameter for single-mode fiber, and 50 to 100 microns for multimode fiber.

CRC (CYCLIC REDUNDANCY CHECK)—A basic error-checking mechanism for link-level data transmissions; a characteristic link-level feature of (typically) bit-oriented data communications protocols. The data integrity of a received frame or packet is checked via a polynomial algorithm based on the content of the frame, and then matched with the result obtained by the sender and included in a (most often, 16-bit) field appended to the frame.

CSMA/CD (CARRIER SENSE MULTIPLE ACCESS/COLLISION DETECTION)—A local area network access method in which contention between two or more stations is resolved by collision detection. When two stations transmit at the same time, they both stop and signal that a collision has occurred. Each then tries again after waiting a predetermined time period, usually several microseconds.

CSU (CHANNEL SERVICE UNIT)—A component of customer premises equipment used to terminate a digital circuit (such as DDS or T1) at the customer site; performs certain line-conditioning functions, ensures network compliance with FCC rules, and responds to loopback commands from the central office; also, ensures proper "ones" density in transmitted bit stream and corrects bipolar violations (also see DSU).

COTR—Contracting Officers Technical Representative

D

D4 FRAMING—A T1 12-frame format in which the 93rd bit is used for framing and signaling information; ESF is an equivalent but newer 24-frame technology.

DAA—Designated Approval Authority

DADPSSO—Division/Department ADP Security Officer

DARPA—see ARPA

DATA—Information represented in digital form, including voice, text, facsimile, and video.

DATA COMMUNICATIONS—The transmission, reception, and validation of data; data transfer between data source (origin node) and data sink (destination node) via one or more data links according to appropriate protocols.

DATA LINK—Any serial data-communications transmission path, generally between two adjacent nodes or devices and without intermediate switching nodes. A data link includes the physical transmission medium, the protocol, and associated devices and programs, so it is both a physical and a logical link.

DATA-LINK LAYER—Layer Two in the OSI model; the network processing entity that establishes, maintains, and releases data-link connections between (adjacent) elements in a network; controls access to the physical medium (Layer One).

DATA-TRANSFER RATE—The average number of bits, characters, or blocks per unit of time transferred from a data source to a data sink.

DATAGRAM—A finite-length packet with sufficient information to be independently routed from source to destination; datagram transmission typically does not involve end-to-end session establishment and may or may not entail delivery-confirmation acknowledgment.

DCE (DATA COMMUNICATIONS EQUIPMENT)—Devices that provide the functions required to establish, maintain, and terminate a data-transmission connection; e.g., a modem.

DCI—Director of Central Intelligence

DDS (DATAPHONE DIGITAL SERVICE)—A private line digital service offered intraLATA by BOCs (Bell Operated Companies) and interLATA by AT&T Communications, with data rates typically at 2.4, 4.8, 9.6, and 56 Kbps; part of the services listed by AT&T under the Accunet family.

DDS-SC—Dataphone® Digital Service with Secondary Channel, also referred to as DDS II, a tariffed private-line service offered by AT&T and certain Bell Operated Companies (BOCs) that allows 64-Kbps clear-channel data with a secondary channel providing end-to-end supervisory, diagnostic, and control functions.

DECnet®—Digital Equipment Corporation's proprietary network architecture that works across all of the company's machines; endowed with a peer-to-peer methodology.

DEDICATED LINE—A dedicated circuit, a nonswitched channel; also called a private line; see leased line.

DELAY—In communications, the time between two events; see propagation delay, and response time.

DES (DATA ENCRYPTION STANDARD)—A scheme approved by the National Bureau of Standards that encrypts data for security purposes. DES is the data communications encryption standard specified by Federal Information Processing Systems (FIPS) Publication 46.

DESTINATION FIELD—A field in a message header that contains the address of the station to which a message is being directed.

DIGITAL—Referring to communications procedures, techniques, and equipment by which information is encoded as either a binary one (1) or zero (0); the representation of information in discrete binary form, discontinuous in time; compare with analog.

DISA—Defense Information Systems Agency

DISK/FILE SERVER—A mass-storage device that can be accessed by several computers; enables the storage and sharing of files.

DISTRIBUTION FRAME—A wallmounted structure for terminating telephone wiring, usually the permanent wires from or at the telephone central office, where cross-connections are readily made to extensions; also called "distribution block."

DLC (DATA LINK CONTROL)—The set of rules (protocol) used by two nodes, or stations, on a network to perform an orderly exchange of information.

DMA (DIRECT MEMORY ACCESS)—A method of moving data from a storage device to RAM.

DNA (DIGITAL NETWORK ARCHITECTURE)—Digital Equipment Corporation's layered data communications protocol.

DNIC (DATA NETWORK IDENTIFICATION CODE) —A four-digit number assigned to public data networks and to specific services within those networks.

DOMAIN—see Apollo DOMAIN

DOS (DISK OPERATING SYSTEM)—A set of programs that instruct a disk-based computing system to manage resources and operate related equipment.

DOWNTIME—The period during which computer or network resources are unavailable to users because of a failure.

DRAFT PROPOSAL—An ISO standards document that has been registered and numbered but not yet given final approval.

DRIVER—A software module that, under control of the processor, manages an I/O port to an external device (e.g., a serial RS-232C port to a modem).

DROP CABLE—In local area networks, a cable that connects the main network cable, or bus, and the data terminal equipment (DTE).

DSI—Defense Simulation Internet

DSU (DATA SERVICE UNIT)—A component of customer premises equipment used to interface to a digital circuit (say, DDS or T1), combined with a channel service unit (CSU); converts a customer's data stream to bipolar format for transmission.

DTE (DATA TERMINAL EQUIPMENT)—User devices, such as terminals and computers, that connect to data circuit-terminating equipment such as modems; they either generate or receive the data carried by the network; in RS-232C connections, designation as either DTE or DCE determines the signaling role in handshaking; in a CCITT X.25 interface, the device or equipment that manages the interface at the user premises; see DCE.

E

EBCDIC (EXTENDED BINARY CODED DECIMAL INTERCHANGE CODE)—An 8-bit character code used primarily in IBM® equipment; the code provides for 256 different bit patterns; compare with ASCII.

EIA (ELECTRONIC INDUSTRIES ASSOCIATION)—A standards organization in the U.S.A. specializing in the electrical and functional characteristics of interface equipment.

EISA (EXTENDED INDUSTRY STANDARD ARCHITECTURE) BUS—A 32-bit adaptation of the 8- and 16-bit buses originally developed by IBM® and now standard in almost all PCs that use Intel® 8086, 80286, and 80386 microprocessors. The EISA bus is a joint development of COMPAQ® and other PC manufacturers; compare with Micro Channel®.

EMI (ELECTROMAGNETIC INTERFERENCE)—A device's radiation leakage that couples onto a transmission medium, resulting (mainly) from the use of high-frequency-wave energy and signal modulation; reduced by shielding; minimum acceptable levels are detailed by the FCC, based on type of device and operating frequency.

EMR—Electromagnetic radiation

EMULATION—The imitation of all or part of one device, terminal, or computer by another, so that the imitating device accepts the same data, performs the same functions, and appears to other network devices as if it were the imitated device.

ENCODING/DECODING—The process of organizing information into a format suitable for transmission, and then reconverting it after transmission; for pulsecode-modulated voice transmission, the generation of digital signals to represent quantified samples, and the subsequent reverse process.

EPROM (ERASABLE PROGRAMMABLE READ-ONLY MEMORY)—See ROM.

ERASABLE STORAGE—A storage device whose contents can be modified (e.g., Random Access Memory, or RAM), as contrasted with read-only storage (e.g., Read-Only Memory, or ROM).

ESCORTS—Escorts are duly designated personnel who have appropriate clearances and access authorization for material contained in an area. They are sufficiently knowledgeable in the security implications of, and control of the activities and access of the individual(s) being escorted.

ETHERNET—A popular local area network design, the product of Xerox® Corp., characterized by 10-Mbps baseband transmission over a shielded coaxial cable and employing CSMA/CD as the access control mechanism, standardized by the IEEE as specification IEEE 802.3; referring to the Ethernet design or as compatible with Ethernet.

F

FCC (FEDERAL COMMUNICATIONS COMMISSION)—Board of commissioners appointed by the President under the Communications Act of 1934, with the authority to regulate all interstate telecommunications originating in the United States.

FCS (FRAME CHECK SEQUENCE)—In bit-oriented protocols, a 16-bit field that contains transmission error checking information, usually appended at the end of a frame.

FDDI (FIBER DISTRIBUTED DATA INTERFACE) (ANSI X.3T9)—An American National Standards Institute (ANSI) specified standard for fiber optic links with data rates up to 100 Mbps. The standard specifies: multimode fiber; 50/125, 62.5/125, or 85/125 core-cladding specification; an LED or laser light source; and 2 kilometers for unrepeated data transmission.

FDO—Foreign Disclosure Office (Navy ITO)

FEP (FRONT-END PROCESSOR)—A dedicated computer linked to one or more host computers or multiuser minicomputers; performs data-communications functions and serves to off-load the attached computers of network processing; in IBM® SNA networks, an IBM® 3704, 3705, 3725, or 3745 communications controller.

FIBER LOSS—The attenuation (deterioration) of the light signal in optical-fiber transmission.

FIBER OPTICS—Transmission technology in which modulated light wave signals, generated by a laser or LED, are propagated along a (typically) glass or plastic medium, and then demodulated to electrical signals by a light-sensitive receiver.

FILE SERVER—In local area networks, a station dedicated to providing file and mass data storage services to the other stations on the network.

FLAG—In communications, a bit pattern of six consecutive "1" bits (character representation is 01111110)

used in many bit-oriented protocols to mark the beginning (and often the end) of a frame.

FLOW CONTROL—The procedure or technique used to regulate the flow of data between devices; prevents the loss of data once a device's buffer has reached its capacity.

FOIRL—Fiber Optic Inter Repeater Link

FRACTIONAL T1 (FT1)—A flexible and upgradable digital communication link that provides a portion of one 1.544-megabit T1 service.

FRAME RELAY—Frame Relay is an emerging interface standard whose first application will be the integration of voice and data traffic on private T1 backbones. Jointly developed by the CCITT and ANSI, Frame Relay is a connection-oriented network that forms permanent virtual circuits.

FRAMING—A control procedure used with multiplexed digital channels, such as T1 carriers, whereby bits are inserted so that the receiver can identify the time slots that are allocated to each sub channel; framing bits may also carry alarm signals indicating specific alarm conditions.

FTAM (FILE TRANSFER, ACCESS, AND MANAGEMENT)—An OSI application utility that provides transparent access to files stored on dissimilar systems.

FTP (FILE TRANSFER PROTOCOL)—An upper-level TCP/IP service that allows copying of files across a network.

G

GAIN—Increased signal power, usually the result of Amplification; see attenuation.

GATEWAY—A conceptual or logical network station that serves to interconnect two otherwise incompatible networks, network nodes, subnetworks, or devices; performs a protocol-conversion operation across numerous communications layers.

GCB—General Communications Backbone. The non-secure, Level II corporate network backbone for NRaD. Consists of broadband, ethernet and FDDI technologies.

GOSIP—Government Open Systems Interconnection Profile. GOSIP defines a common set of OSI data communication protocols which enable computer systems within the U.S. Government from multiple vendors to interact and enable users of diverse applications to exchange information.

GPIB—General Purpose interface bus

GROUND—An electrical connection or common conductor that, at some point, connects to the earth.

GROUP ADDRESSING—In transmission, the use of an address that is common to two or more stations; on a multipoint line, where all stations recognize addressing characters, but only one station responds.

H

HEAD END—A passive component in a broadband transmission network that translates one range of frequencies (Transmit) to a different frequency band (Receive); allows devices on a single cable network to send and receive signals without interference.

HEADER—The control information added to the beginning of a message; contains the destination address, source address, and message number.

I

IATO—see Interim Authority to Operate

ICMP (Internet CONTROL MESSAGE PROTOCOL) —The TCP/IP process that provides the set of functions used for networking layer management and control.

IDOCS (INTRUSION DETECTION OPTICAL COMMUNICATIONS SYSTEM)—IDOCS is a National Security Agency (NSA) approved communications network link developed by Hughes Aircraft Company for the transfer of classified data at Ethernet speeds. IDOCS can transfer up to secret level data. IDOCS is based upon a specially designed fiber optic cable. The IDOCS cable uses scattered light carried by an outer conductor to shield the inner conductor. The inner conductor carries the data. By constantly monitoring the outer conductor signal strength or attenuation you can tell when the cable has been damaged or compromised. If the signal strength is not correct, the Fiber Alarmed Modems (FAM 131s) automatically quits transmitting data and sounds an alarm.

IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS)—An international society of professional engineers that issues widely used networking standards.

IEEE 802.5—see Token Ring

IETF—Internet Engineering Task Force, a non-government standards body that precedes over the Internet community.

IMPEDANCE—The effect on a transmitted signal of resistance, inductance, and capacitance.

INADVERTENT DISCLOSURE—Accidental exposure of classified information to a person not authorized access. This may result in a "compromise" or a need-to-know violation.

INDIVIDUAL ACCOUNTABILITY—Measures to positively associate the identity of a user with their access (time, method and degree) to machines and material.

INFOSEC—Information security

INSIDE WIRING—In telephone deregulation, the customer's premises wiring; the wiring inside a building.

INTEGRITY—The capability of a computer system to perform its intended function in an unimpaired manner. Free from deliberate or inadvertent unauthorized manipulation of the system.

INTELLIGENT TERMINAL—A programmable terminal.

INTERACTIVE PROCESSING—Describing time dependent (real-time) data communications; a user enters data and then awaits a response from the destination before continuing; also, conversational; contrast with batch processing.

INTERFACE—A shared boundary; a physical point of demarcation between two devices, where the electrical signals, connectors, timing, and handshaking are defined; the procedures, codes, and protocols that enable two entities to interact for a meaningful exchange of information.

INTERNATIONAL STANDARD—An ISO standards document that has been approved in final balloting.

Internet®—A large network comprised of several smaller networks.

I/O—Input/Output.

IP (Internet PROTOCOL)—Used in gateways to connect networks at the OSI network layer (Layer 3 and above).

IPO—International Programs Office

IPX—Protocol used by the Netware network operating system.

ISDN (INTEGRATED SERVICES DIGITAL NETWORK)—A project within the CCITT for the standardization of operating parameters and interfaces for a network that will accommodate a variety of mixed digital transmission services; access channels under definition include basic rate (144 Kbps) and primary rates (nominally, 1.544 and 2.048 Mbps).

ISO (INTERNATIONAL STANDARDS ORGANIZATION)—An organization that promotes the development of standards for computers; developer of the OSI model.

J

JITTER—The slight movement of a transmission signal in time or phase that can introduce errors and loss of synchronization in high-speed synchronous communications.

JUMPER—A patch cable or wire used to establish a circuit, often temporarily, for testing or diagnostics.

K

k—Kilo; notation for one thousand (e.g., Kbps).

K—See kilobyte.

Kbps—Kilobits per second; standard measurement of data rate and transmission capacity. One Kbps equals 1000 bits per second.

KG—Designator for cryptological unit. Common KGs in use today are the KG-84A (56-64 Kbps) and the KG-94 / KG-194 (T1 speeds)

KILOBYTE—Standard quantity measurement for disk and diskette storage: One K equals 1024 bytes (8-bit characters) of memory.

L

LAN (LOCAL AREA NETWORK)—A type of highspeed data-communications arrangement where all segments of the transmission medium (coaxial cable, twisted-pair wire, or optical fiber) are in an office or campus environment under the control of the network operator.

LAN MANAGER—Proprietary PC network operating system from Microsoft®.

LAP (LINK ACCESS PROCEDURE)—The data-link level protocol specified in the CCITT X.25 interface standard; original LAP has been supplemented with LAPB (LAP-Balanced) and LAPD.

LAPD (LINK ACCESS PROCEDURE-D)—Link-level protocol devised for ISDN connections, differing from LAPB (LAP-Balanced) in its framing sequence. Likely to be used as basis for LAPM, the proposed CCITT modem error-control standard.

LAT (LOCAL AREA TRANSPORT)—A protocol unique to Digital Equipment Corporation products, for virtual terminal access across an Ethernet network.

LATENCY—The time interval between when a network station seeks access to a transmission channel and when access is granted or received; equivalent to waiting time.

LAYER—In the OSI reference model, one of seven basic layers, referring to a collection of related network processing functions; one level of a hierarchy of functions.

LCM—Life cycle management

LEASED LINE—A dedicated circuit, typically supplied by the telephone company, that permanently interconnects two or more user locations; generally voice grade in capacity and in range of frequencies supported; typically analog, though sometimes it refers to DDS subrate digital channels (2.4 to 9.6 Kbps); used for voice (2000 Series leased line) or data (3002 type); could be point-to-point or

multipoint; may be enhanced with line conditioning; also, private line.

LED (LIGHT-EMITTING DIODE)—A device that accepts electrical signals and converts the energy to a light signal; with lasers, the main light source for optical-fiber transmission; used mainly with multimode fiber.

LINK LAYER—Layer Two of the OSI reference model; also known as the Data-Link Layer.

LLC (LOGICAL LINK CONTROL)—A protocol developed by the IEEE 802 committee for data-link-level transmission control; the upper sublayer of the IEEE Layer 2 (OSI) protocol that complements the MAC protocol; IEEE standard 802.2; includes end-system addressing and error checking.

LOSS—Reduction in signal strength, expressed in decibels; also, attenuation; opposite of gain.

LSI (LARGE-SCALE INTEGRATION)—A term used to describe a multifunction semiconductor device, such as a microprocessor, with a high density of electronic circuitry on a single silicon chip (up to 1000 circuits).

LU 6.2—In SNA, a set of protocols that provides peer-to-peer communications between applications.

M

m—Milli; designation for one thousandth.

M—Mega; designation for one million (e.g., Mbps).

M BIT—The More Data mark in an X.25 packet that allows the DTE or DCE to indicate a sequence of more than one packet.

MAC (MEDIA ACCESS CONTROL)—A media specific access-control protocol within IEEE 802 specifications; currently includes variations for the Token Ring, token bus, and CSMA/CD; the lower sublayer of the IEEE's Link Layer (OSI), which complements the Logical Link Control (LLC).

MAGNETIC MEDIUM—Any data-storage medium and related technology, including disks, diskettes, an tapes, in which different patterns of magnetization represent bit values.

MANCHESTER ENCODING—Digital encoding technique (specified for the IEEE 802.3 Ethernet baseband network standard) in which each bit period is divided into two complementary halves; a negative-to-positive (voltage) transition in the middle of the bit period designates a binary "1," while a positive-to-negative transition represents a "0." The encoding technique also allows the receiving device to recover the transmitted clock from the incoming data stream (self-clocking).

MAP (MANUFACTURING AUTOMATION PROTOCOL)—A General Motors® originated suite of networking protocols, the implementation of which tracks the seven layers of the OSI model.

MAPPING—In network operations, the logical association of one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network (e.g., name-address internetwork route, protocol-to-protocol mapping).

MAU (MULTISTATION ACCESS UNIT)—A wiring concentrator used in local area networks.

MEDIUM—Any material substance used for the propagation or transmission of signals, usually in the form of electrons or modulated radio, light, or acoustic waves; examples include optical fiber, cable, wire, dielectric slab, water, air, or free space.

MEGABYTE—Mbyte, Meg, or MB, 1,048,576 bytes, equivalent of 1024 kilobytes; basic unit of measurement of mass storage; also used in describing data transfer rates (primarily parallel) as a function of time (e g, Mbps).

MHS (MESSAGE HANDLING SYSTEM)—The standard defined by the CCITT as X.400 and by the ISO as Message Oriented Text Interchange Standard (MOTIS)

Micro Channel®—A proprietary bus developed by IBM® for its PS/2® family of computers' internal expansion cards; also offered by Tandy® and other vendors. Compare with EISA bus.

MICROPROCESSOR—An electronic integrated circuit, typically a single-chip package, capable of receiving and executing coded instructions. For example, Zilog Z80, Intel® 8088, and Motorola® 68000 are popular microprocessors.

MIF (MINIMUM INTERNETWORKING FUNCTIONALITY)—A general principle within the ISO that calls for minimum local-area-network station complexity when interconnecting with resources outside the local area network.

MINI-MAP (MINI-MANUFACTURING AUTOMATION PROTOCOL)—A version of MAP consisting of only physical, link, and application layers, intended for lower-cost process-control networks. With Mini-MAP, a device with a token can request a response from an addressed device; unlike a standard MAP protocol, the addressed Mini-MAP device need not wait for the token to respond.

MIPS (MILLION INSTRUCTIONS PER SECOND)—A general comparison gauge of a computer's raw processing power.

MIS—Management Information System

MLS—Multi-level security

MOA—Memorandum of Agreement

MODEM (MOdulator/DEModulator)—A device that converts between serial streams of data and analog waveforms suitable for transmission on a telephone line.

MS® OS/2® LAN MANAGER—The multiuser network operating system codeveloped by Microsoft® and 3Com®. LAN Manager offers a wide range of network management and control capabilities unavailable with existing PC-based network operating systems.

MS-DOS® (MICROSOFT DISK OPERATING SYSTEM) —Microcomputer operating system developed for the IBM® PC and hence, a de facto industry standard; also referred to as PC-DOS, primarily by IBM®.

MTBF (MEAN TIME BETWEEN FAILURES)— A stated or published period of time for which a user may expect a device to operate before a failure occurs.

MTTR (MEAN TIME TO REPAIR)—The average time required to perform corrective maintenance on a failed device.

MULTIMODE—Essentially, an optical fiber designed to carry multiple signals, distinguished by frequency or phase, at the same time; compare with single mode.

MULTIPLE ROUTING—The process of sending a message to more than one recipient, usually when all destinations are specified in the header of the message.

MULTIPOINT LINE—A single communications line or circuit interconnecting several stations supporting terminals in several different locations. This type of line usually requires some kind of polling mechanism, each terminal having a unique address. Also called a multidrop line.

MULTITASKING—The concurrent execution of two or more tasks or applications by a computer; may also be the concurrent execution of a single program that is used by many tasks.

N

NANOSECOND—One billionth of a second.

NCC (NETWORK CONTROL CENTER)—Any centralized network diagnostic and management station or site, such as that of a packet-switching network.

NCSC—National Computer Security Council

NDIS (NETWORK DRIVER INTERFACE SPECIFICATION)—A standard established by Microsoft® for writing hardware-independent drivers.

NES®—Motorola Network Encryption Unit, an ethernet network to ethernet network encryption device.

NETBIOS (NETWORK BASIC INPUT/OUTPUT SYSTEM)—Software developed by IBM®; provides the interface between a PC's operating system, the I/O bus, and the network; a de facto network standard.

NETVIEW®—An IBM® mainframe network management product that integrated the functions of several earlier IBM® network management products.

NETWORK—An interconnected group of nodes; a series of points, nodes, or stations connected by communications channels; the assembly of equipment through which connections are made between data stations.

NETWORK ARCHITECTURE—A set of design principles, including the organization of functions and the description of data formats and procedures, used as the basis for the design and implementation of a network (ISO).

NETWORK INTERFACE CONTROLLER—Electronic circuitry that connects a workstation to a network, usually in the form of a card that fits into one of the expansion slots inside a personal computer. It works with the network software and computer operating system to transmit and receive messages on the network; also, "network interface card."

NETWORK LAYER—Layer Three in the OSI model; the logical network entity that services the transport layer; responsible for ensuring that data passed to it from the transport layer is routed and delivered through the network.

NETOP—NETwork Operating Procedures

NETSPPH—NETwork Security Policy and Plans Handbook

NETWARE®—A proprietary network operating system sold by Novell Inc. Currently has the largest market share in the workstation networking arena. Supports PCs running DOS and Windows, OS/2, Macs, and UNIX NFS compatible machines.

NETWORK TOPOLOGY—The physical and logical relationship of nodes in a network; the schematic arrangement of the links and nodes of a network; networks typically have a star, ring, tree, or bus topology, or some hybrid combination.

NFS—Network File System, a specification for accessing files over a network, created by SUN Microsystems®, Inc., for UNIX workstations over TCP/IP networks. The specification has been released to the open market and has been standardized by the IETF. Some vendors have even ported NFS to on UNIX machines such as MS-DOS® PCs and Macs.

NFS (NETWORK FILE SERVER)—An extension of TCP/IP that allows files on remote nodes of a network to appear locally connected.

NIC—Navy Intelligence Command

NODE—A point where one or more functional units interconnect transmission lines, a physical device that allows for transmission of data within a network; includes

host processors, communications controllers, cluster controllers, and terminals.

NSA—National Security Agency

NSM—Network Security Manager

NSO—Network Security Officer

O

OFF LINE—Condition in which a user, terminal, or other device is not connected to a computer or is not actively transmitting via a network.

ON LINE—Condition in which a user, terminal, or any device is actively connected with the facilities of a communications network or computer; opposite of off line.

OP—Operating Procedures - See NETOP

OPERATING SYSTEM—The software of a computer that controls the execution of programs, typically handling the functions of input/output control, resource scheduling, and data management (e.g., CP/M®, MS-DOS®, VM/370). An integrated collection of service routines for supervising the sequence and processing of programs by a computer.

OPR—Officers of Primary Responsibility

OPTICAL DISK—A very-high-density information storage medium that uses light to read and write digital information.

OPTICAL FIBER—Any filament or fiber, made of dielectric materials, that is used to transmit laser- or LED-generated light signals; optical fiber usually consists of a core, which carries the signal, and cladding, a substance with a slightly higher refractive index than the core, which surrounds the core and serves to reflect the light signal.

OSI (OPEN-SYSTEM INTERCONNECTION)—A logical structure (model) for network operations standardized within the ISO, a seven-layer network architecture being used for the definition of network protocol standards to enable any OSI-compliant computer or device to communicate with any other OSI-compliant computer or device for a meaningful exchange of information; the layers are: Physical, Data Link, Network, Transport, Session, Presentation, Application.

OSINET—A test network, sponsored by the National Bureau of Standards (NBS), designed to provide vendors of products based on the OSI model a forum for doing interoperability testing.

OS/2®—The third-generation operating system developed by IBM® and Microsoft® for use with the Intel® 80286 and 80386 microprocessors. Unlike its predecessor (PC MS-DOS), OS/2 is a multitasking operating system. OS/2 also refers to operating software that will run on the Personal System/2®. OS/2 Standard Edition® is a joint Microsoft® and IBM® development, while OS/2 Extended Edition® is the IBM® proprietary extension to include communications and database managers.

OVERHEAD—In communications, all information, such as control, routing, and error-checking characters, that is in addition to user-transmitted data; includes information that carries network status or operational instructions, network routing information, and retransmissions of user data messages that are received in error.

P

PACKET—A sequence of data, with associated control information, that is switched and transmitted as a whole; refers mainly to the field structure and format defined with the CCITT X.25 recommendation.

PARALLEL PROCESSING—Concurrent or simultaneous execution of two or more processes, or programs, within the same processor, as contrasted with serial or sequential processing.

PASS-THROUGH—The ability to gain access to one network element through another.

PASSIVE DEVICE—In current loop applications, a device that must draw its current from connected equipment.

PBX (PRIVATE BRANCH EXCHANGE)—A manual, user-owned telephone exchange.

PC (PERSONAL COMPUTER)—A generic term for a single-user microcomputer; PC also refers to the IBM® Personal Computer, the first microcomputer to be widely accepted in business and still a standard for compatibility.

PDS—Protective distribution system

PENETRATION—The successful unauthorized access into a system.

PHYSICAL CONTROL ZONE—The space or area surrounding equipment processing classified information which is under sufficient physical and technical control to prevent a successful hostile intercept of any classified information from within such space or areas.

PHYSICAL LAYER—Within the OSI model, the lowest level (Level One) of network processing, below the link layer; concerned with the electrical, mechanical, and handshaking procedures over the interface that connects a device to a transmission medium; referring to an electrical interface, such as RS-232C.

PIXEL (PICTURE ELEMENT)—smallest unit of a graphics or video display; light characteristics (color and intensity) which can be coded into an electrical signal for transmission.

POINT-TO-POINT—Describing a circuit that interconnects two points directly, where there are generally no intermediate processing nodes, computers, or branched circuits, although there could be switching facilities; a type

of connection, such as a phone line circuit, that links two, and only two, logical entities; see broadcast.

POLARITY—Any condition in which there are two opposing voltage levels or changes, such as positive and negative.

PORT—A point of access into a computer, a network, or other electronic device; the physical or electrical interface through which one gains access; the interface between a process and a communications or transmission facility.

POSIX—Portable Operating System for Computer Environments

POTS—Plain Old Telephone System

PRESENTATION LAYER—Layer Six of the ISO reference model; provides standards for restructuring data into the required format, character set, or language.

PRIMITIVES—Basic units of machine instruction.

PRINT SERVER—An intelligent device used to transfer information to a series of printers.

PROPAGATION DELAY—The time it takes a signal composed of electromagnetic energy to travel from one point to another over a transmission channel; usually most noticeable in communicating with satellites; normally, the speed-of-light delay.

PROTOCOL—Formal set of rules governing the format, timing, sequencing, and error control of exchanged messages on a data network; may be oriented toward data transfer over an interface, between two logical units directly connected, or on an end-to-end basis between two users over a large and complex network.

PS/2® (PERSONAL SYSTEM/2®)—The IBM® current family of microcomputers that, with OS/2®, represents a higher level of performance, capacity, and software consistency than the firm's previous microcomputers, the IBM® PCs.

PUBLIC NETWORK—A network operated by common carriers or telecommunications administrations for the provision of circuit-switched, packet-switched, and leased-line circuits to the public.

Q

QUEUE—Any group of items, such as computer jobs or messages, waiting for service.

QUEUING—Sequencing of batch data sessions.

R

RAM (RANDOM ACCESS MEMORY)—Storage device into which data can be entered (written) and read; compare with ROM.

REAL-TIME—Operating mode that allows immediate interaction with data as it is created, as in a process control system or computer-aided design system.

REDUNDANCY—In data transmission, the portion of a message's gross information content that can be eliminated without losing essential information; also, duplicate facilities.

REPEATER—In digital transmission, equipment that receives a pulse train, amplifies it, retimes it, and then reconstructs the signal for retransmission; in fiber optics, a device that decodes a low-power light signal, converts it to electrical energy, and then retransmits it via an LED or laser light source; also, regenerative repeater.

RESIDUE—Data left in computer memory or storage after use.

RESPONSE TIME—For interactive sessions, the elapsed time between the end of an inquiry and the beginning of a response.

RETRANSMISSIVE STAR—In optical-fiber transmission, a passive component that permits the light signal on an input fiber to be retransmitted on multiple output fibers; formed by heating together a bundle of fibers to near the melting point; used mainly in fiber based local area networks; also, star coupler.

RING NETWORK—A network topology in which each node is connected to two adjacent nodes.

RISC (REDUCED INSTRUCTION SET COMPUTING)—Internal computing architecture where processor instructions are pared down so that most can be performed in a single processor cycle, theoretically improving computing efficiency.

ROM (READ-ONLY-MEMORY)—A data storage device, the contents of which cannot normally be altered; storage in which writing-over is prevented; also, permanent storage; compare with RAM.

ROUTER—A network device that examines data addresses; determines the most efficient pathway to the destination, and routes the data accordingly.

ROUTING—The process of selecting the correct circuit path for a message.

S

SAA (SYSTEM APPLICATION ARCHITECTURE)—A set of standards developed by IBM®, providing identical user interfaces for applications running on PCs, minicomputers, and mainframes.

SAFENET—Survivable Adaptable Fiber Optic Embedded Network

SCI—Sensitive Compartmented Information

SECURITY INCIDENT—Any incident involving classified information in which there is a deviation from the requirements of governing security regulations (compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples).

SECURITY TEST AND EVALUATION—An examination and analysis of the security features of a computer system as they have been applied in an operational environment to develop factual evidence upon which an accreditation can be based.

SERIAL TRANSMISSION—The sequential transmission of the bits constituting an entity of data over a data circuit.

SESSION—A connection between two stations that allows them to communicate; the time period that a user engages in a dialogue with an interactive computer; in the IBM® SNA, the logical connection between two network-addressable units.

SESSION LAYER—Layer Five of the OSI reference model; provides protocols for assembling physical messages into logical messages.

SHIELDING—Protective enclosure surrounding a transmission medium, such as coaxial cable, designed to minimize electromagnetic leakage and interference.

SINGLE MODE—Describing an optical wave guide designed to propagate light of only a single wavelength and perhaps a single phase; essentially, an optical fiber that allows the transmission of only one light beam, or data-carrying lightwave channel, and is optimized for a particular lightwave frequency; compare with multimode.

SMDS—Switched Multimegabit Data Service (SMDS) will be a nationwide service for transmitting data among remote locations over a packet-switched wide area network. Its goal is to extend the low-delay and high-bandwidth performance of LANs to the metropolitan area. The specification is based on a connectionless datagram service at T1 and T3 speeds by the mid-1990s. Greater speeds are also planned for deployment on SONET.

SNA® (SYSTEMS NETWORK ARCHITECTURE)—The IBM® network architecture for communications among IBM® devices, and between IBM® and other machines.

SNMP—Simple Network Management Protocol

SONET (SYNCHRONOUS OPTICAL NETWORK)—An emerging hierarchical high speed multiplexing international standard that will allow the communications carriers to exploit the huge installed base of fiber optic cable installed across the country. The OC-3 or Optical Connection 3 level of the SONET hierarchy, operating at 155Mbits/s is the first operational speed that will probably be offered.

SOP—Standard Operating Procedures

SPOOL (SIMULTANEOUS PERIPHERAL OPERATION ON LINE)—A program or piece of hardware that controls data going to an output device.

SPPH—Security Policy and Plans Handbook - see NETSPPH.

ST—Stream Protocol. Simulation protocol used on the DSI network.

STAR TOPOLOGY—The point-to-point wiring of network elements to a central node.

STARLAN—A local area network design and specification, within the IEEE 802.3 standards, characterized by 1-Mbps baseband data transmission over two-pair twisted-pair wiring.

STATION—Any DTE that receives or transmits messages on a data link, including network nodes and user devices.

STEP-INDEX—A type of optical fiber with a uniform refractive index at its core and a sharp decrease in the refractive index at its core-cladding interface.

SYSTEM HIGH SECURITY MODE—The mode of operation in which system hardware / software is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all the components electrically or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed.

T

T CARRIER—A time-division-multiplexed, digital transmission facility, typically telephone-company supplied, usually operating at an aggregate data rate of 1.544 Mbps and above.

T1—AT&T term for a digital carrier facility used to transmit a DS-1 formatted digital signal at 1.544 Mbps.

T3—Telecommunications service with a bandwidth of 45 Mbps. Typically broken into 23-27 T1 circuits.

TASO—Terminal Area Security Officer

TCP/IP (TRANSMISSION CONTROL PROTOCOL Internet® PROTOCOL)—A layered set of protocols that allows sharing of applications among PCs in a high-speed communications environment. Because TCP/IP's protocols are standardized across all its layers, including those that provide terminal emulation and file transfer, different vendors' computing devices (all running TCP/IP) can exist on the same cable and communicate with one

another across that cable. Corresponds to Layers Four (transport) and Three (network) of the OSI reference model.

TDM—Time Division Multiplex

TELCO—Telephone central office, in most usage's; hut also, a generic abbreviation for "telephone company."

TELECOMMUNICATIONS—A term encompassing both voice and data communications in the form of coded signals over media.

Telenet®—A virtual terminal service available through the TCP/IP protocol suite.

TEMPEST—Investigation and study of compromising emanations.

10Base2—IEEE 802.3 10 Mbps ethernet standard also called Thinwire or Cheapernet. Allows distances of 185m and 20 devices per unrepeated segment over RG-58 coax cable with BNC connection to the network device.

10Base5—IEEE 802.3 10 Mbps ethernet standard also called Thickwire. Allows distances of 500m per unrepeated segment over RG-36 coax cable.

10BaseT—IEEE 802.3 10 Mbps ethernet standard over twisted pair copper wire (both shielded and unshielded). The topology is a star radiating from a concentrator hub. The maximum distance from a node from the hub is 100m.

10BaseF—IEEE 802.3 10 Mbps ethernet standard over fiber optic cable. Specification consists of three portions: 1) 10BaseFL - connections to a workstation or network node up to 2 km; 10BaseFP - specification using passive splitter hubs; and 10BaseFS - synchronous hub technology that eliminates the "four repeater" rule (in ethernet, no more than four repeaters can exist between the two farthest devices on a physical segment).

10Broad36—IEEE 802.3 10 Mbps ethernet standard over a broadband CATV network. The farthest distance between to nodes on the network is 3600m

TERMINAL—Point in a network at which data can either enter or leave; a device, usually equipped with a keyboard, often with a display, capable of sending and receiving data over a communications link; generically the same as data terminal equipment (DTE).

TERMINAL SERVER—A device that allows one or more terminals or other devices to connect to an Ethernet.

TERMINATED LINE—A circuit with a resistance at the far end equal to the characteristic impedance of the line, so no reflections or standing waves are present when a signal is entered at the near end.

TEXT—In communications, transmitted characters forming the part of a message that carries information to be conveyed; in some protocols, the character sequence between start-of-text (STX) and end-of-text (ETX) control characters; information for human, as opposed to computer, comprehension, intended for presentation in a two-dimensional form.

THICKWIRE—see 10Base5

THINWIRE—see 10Base2

TIMEOUT—Expiration of predefined time period, at which point some specified action occurs; in communications, timeouts are employed to avoid unnecessary delays and improve traffic flow; used, for example, to specify maximum response times to polling and addressing before a procedure is automatically reinitiated.

TOKEN BUS—A LAN standard that uses a token passing media access method on a bus configuration.

TOKEN RING—A data-signaling scheme, such as IEEE 802.5/Token Ring or FDDI, in which a special data packet (called a token) is passed from one station to another along an electrical ring. When a station wants to transmit, it takes possession of the token, transmits its data, then frees the token after the data has made a complete circuit of the electrical ring.

TOP (TECHNICAL AND OFFICE PROTOCOLS)—A Boeing version of the MAP protocol suite, aimed at office and engineering applications.

TOPOLOGY—See network topology.

TRANSACTION—In communications, a message destined for an application program; a computer processed task that accomplishes a particular action or result; in interactive communications, an exchange between two devices, one of which is usually a computer; in batch or remote job entry, a job or job step.

TRANSCEIVER—A device that can both transmit and receive.

TRANSMISSION—The dispatching of a signal, message, or other form of intelligence by wire, radio, telegraphy, telephony, facsimile, or other means; a series of characters, messages, or blocks, including control information and user data; the signaling of data over communications channels.

TRANSPORT LAYER—Layer Four in the OSI reference model; provides a logical connection between processes on two machines.

TREE—A LAN topology that recognizes only one route between two nodes on the network. The "map" resembles a tree or the letter T.

TRUNK—A dedicated aggregate telephone circuit connecting two switching centers, central offices, or data-concentration devices.

TSO—TEMPEST Security Officer

TWISTED PAIR—Two insulated copper conductors that are wound around each other, mainly to cancel the effects of electrical noise; typical of standard telephone wiring; unshielded twisted pair contains no outside wrap-around conductor.

U

UDP (USER DATAGRAM PROTOCOL)—The TCP/IP transaction protocol used for applications such as remote network management and name-service access; lets users assign a name, such as "VAX®2," to a physical or numbered address.

ULTRAnet®—A proprietary network technology from Ultra Network Technologies (San Jose, Ca.) is a hub-oriented network that will provide high-speed access to supercomputers, mini-supercomputers, mainframes, workstations, graphic visualization stations and networks such as ethernet and FDDI.

UNIX®—Operating system originally designed by AT&T for communicating multiuser, 32-bit minicomputers; has come into wide commercial acceptance because of its predominance in Academia and its programming versatility, AT&T System V Version 3 and Berkeley System Development Version 4.3 are currently popular.

UPS—Uninterruptable Power Supply

USER—Any authorized person, office or staff agency who may directly use, or receive services or material from a computer system.

UTILITY SOFTWARE—Programs that make operation of a PC or a LAN more convenient, including programs to move disk files more easily, diagnostic programs, etc. Compare with application software.

V

VAN (VALUE ADDED NETWORK)—A network whose services go beyond simple switching.

VIRTUAL CIRCUIT—In packet-switching, a network facility that gives the appearance to the user of an actual end-to-end circuit; a dynamically variable network connection where sequential data packets may be routed differently during the course of a "virtual connection"; virtual circuits enable transmission facilities to be shared by many users simultaneously.

VIRTUAL STORAGE—Storage space that may be viewed as addressable main storage, but is actually auxiliary storage (usually peripheral mass storage) mapped into real addresses; amount of virtual storage is limited by the addressing scheme of the computer.

VULNERABILITY—A measurement of (a) the susceptibility of a particular system to a specific attack, and (b) the opportunity available to a hostile source to mount such an attack. A vulnerability is always demonstrable, but may exist independently of a known threat. In general, a description of a vulnerability takes account of those factors under friendly control.

W

WAN—Wide Area Network

WAVELENGTH—Distance between successive peaks of a sine wave.

WIDEBAND— A system in which multiple channels access a medium (usually coaxial cable) that has a large bandwidth, greater than that of a voice-grade channel; typically offers higher-speed data-transmission capability. Also see broadband.

WIRING CLOSET—Central location for termination and routing of on-premises wiring systems.

WORKSTATION—Input/output equipment at which an operator works.

X

X.25—The standard interface for packet-switched data-communications networks, as designated by the Consultative Committee for International Telephony and Telegraphy (CCITT).

XENIX—Microsoft® trade name for a 16-bit microcomputer operating system derived from Bell Laboratories' UNIX.

XNS (XEROX® NETWORK SYSTEMS)—A peer-to-peer protocol developed by Xerox that has been incorporated into several local area networking schemes, including the 3Com® 3+® and 3+Open® network operating systems.

XTP—eXpress Transfer Protocol

APPENDIX F

NRAD NETWORKING PROCESS ACTION TEAM (PAT)

NRaD management, recognizing that guidelines needed to be established for implementation of new networks or restructuring of existing networks, established the Networking Process Action Team (PAT) to review current NRaD policies and recommend new policies, procedures, and guidelines to steer NRaD's future in the areas of networks and communications services. This document is a result of that direction. The Networking PAT was granted the following charter as a guideline for this effort.

CHARTER

As the Navy's preeminent C^3I Center, NRaD is responsible for research, development, test, and evaluation of a broad array of command, control, and communications systems. Communications are a key to the NRaD charter and communications networks represent a robust, flexible, and evolving set of communications standards and applications. Recognizing this, the NRaD Networking PAT was chartered to recommend consistent policies for networking at the Center.

STATEMENT OF CHARTER

The following topics are recommended for PAT action:

- The PAT will follow the network management of both the International Standards Organization (ISO) Model and Government Open Systems Interconnect Profile (GOSIP) with particular emphasis on NRaD topics and requirements.
- Security and configuration practices for general purpose and program specific networks for the Seaside complex (Bldgs. 600, 605, & 606) specifically and center wide in general.
- The PAT will consider networking in the broad areas of R&D versus general purpose applications with expectations as to their NRaD wide applications for the future.
- Due to the complexity of NRaD networking issues, the team will establish processes, priorities, and schedules for the purpose of recommending NRaD network policies.

To achieve these objectives the PAT will

- Review current ISO and GOSIP standards as applicable to the Center
- Review current NRaD policies in regards to networking and security
- Review requirements (both physical and program specific, i.e., performance, etc.) for new networks.
- Match state-of-the-art and existing technologies for the best mix of performance versus security to meet the requirements of the new installation.
- Ensure standards (ISO & GOSIP) are adhered to when implementing new networks.
- Implement policies that will aid in the reduction of costs through the use of cost-effective communications methods.
- Implement policies that permit diverse hardware and software products to be connected to form a unified networking system.
- Provide general policies to enable communications that can be easily installed in various configurations to meet the needs of all users.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1993	FINAL: June 1993

4. TITLE AND SUBTITLE
Network Security Guideline

5. FUNDING NUMBERS

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Command, Control and Ocean Surveillance Center
RDT&E Division
San Diego, CA 92152-5001

8. PERFORMING ORGANIZATION REPORT NUMBER
TD 2519

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Naval Command, Control and Ocean Surveillance Center
RDT&E Division
San Diego, CA 92152-5001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This Network Security Guideline was prepared to assist in understanding how the Command will implement the guidance from numerous security regulations and instructions for a network environment, and to establish network security policies and guidelines at this Command. This document is made up of four chapters and an appendix, that includes Introduction, Network concepts and standards, existing local Network Security Policy, and a quick reference guide for network implementators.

14. SUBJECT TERMS
Network Security

15. NUMBER OF PAGES
209

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT